Virtual Private Networking with SonicWALL Technical e*Training

Comprehensive Services from Your Trusted Security Partner

Additional Information

- A cost-effective, “anytime, anywhere” training solution
- In-depth, self-paced courses that are 6-8 hours in duration
- Available for 90 days after initial activation
- Recommended prerequisite for the Certified SonicWALL Security Administrator (CSSA) course and exam
- List price is $350 USD; Free for SonicWALL Medallion Partners

Course Description:

The *Virtual Private Networking with SonicWALL* e*Training course covers general VPN design concepts and technologies, their application via SonicWALL firewall products, installation, configuration and diagnostics. It also covers a general overview of Cryptography and IPSec implementation. Emphasis is placed upon underlying technologies, common configuration, and troubleshooting issues.

Who Should Attend:

Those persons tasked with the support, installation, deployment or administration of SonicWALL products including: System Administrators, Security staff, Firewall Administrators, Network Engineers, Pre-Sales Engineers, System Engineers, Reseller Support, Installation Consultants. Completion of this course is strongly recommended in preparation to attend the CSSA 1-day Lab Class and complete the CSSA certification exam.

Course Objectives:

Upon completing this training course, participants should be able to:

- Understand VPN and its Underlying Technologies
- Design SonicWALL VPN Solutions
- Explain SonicWALL’s VPN Implementation
- Install SonicWALL-to-SonicWALL VPN
- Understand SonicWALL-to-Other VPN
- Design & Install SonicWALL VPN Client Implementations
- Configure SonicWALL Advanced VPN Features
- Troubleshoot for Common Problems

Prerequisites:

- Basic knowledge of networking concepts including network topologies and an understanding of the OSI model of networking protocol stacks
- Understanding of TCP/IP, network addressing, and subnet masks
- Knowledge of basic router concepts
- This course is a prerequisite for all SonicWALL Instructor-led Training courses.

SONICWALL

Virtual Private Networking with SonicWALL Technical e*Training

Topics Covered in this Course include:

- VPN Foundations
    - Secure Access through the Internet
    - Types of Risks VPN Averts
    - Other Problems VPN Solves
    - How VPNs Work
    - Types of VPNs
- Cryptography Overview
    - Encryption Process
    - Ensuring Privacy
    - Ensuring Authenticity
    - Key Exchange Mechanisms
- Implementing an IPSec VPN
    - Components of IPSec
    - Creating an IPSec Security Association
    - Encryption and Authentication Options
    - IPSec Protocol Details
    - Packet Handling in IPSec
    - IKE Management Protocol
    - IKE Security Associations
    - IKE Details
    - Fragmentation and Routing Issues in IPSec
- VPN Design Considerations
    - Defining a VPN Connection Security Policy
    - Design Considerations
    - Design Options for VPN
- SonicWALL VPN Technical Features
    - VPN Features in SonicOS Standard and Enhanced
    - IPSec Support
    - NAT Traversal
    - VPN Bandwidth management
    - VPN Single Armed Mode
    - RIP Broadcasts for VPN Tunnels
    - Digital Certificates – PKI
    - NetBIOS over VPN
- SonicWALL VPN Configuration
    - Defining Security Associations
    - Create a Manual Key Tunnel (Lab simulation included)
    - Create an IKE Main Mode Tunnel (Lab simulation included)
    - Extended VPN Features in SonicOS Enhanced
        - User-definable Networks
        - Group Access Policies
        - VPN Zones
        - Flexible NAT
        - Gateway Redundancy
    - Extended Authentication (Lab simulation included)
    - Global VPN Settings
- Designing SonicWALL VPN Networks
    - Hub and Spoke VPN
    - Create a hub and Spoke VPN (Lab simulation included)
    - VPN with NAT and Firewall Rules
    - Working with DHCP over VPN
- Global VPN Client
    - Installing the Global VPN Client (Lab simulation included)
    - Group VPN Policy
    - Client Provisioning