VeriSign AUTHORIZED TRAINING CENTER

msctrustgate.com
TRUSTED INTERNET SERVICES

VeriSign Trust Network

Essential Virtual Private Networks (VPN) Components

Length : 3 Days

Overview

Essential VPN Components is a three-day course designed to give IT professionals the insight and information they need to make informed decisions regarding the planning, design, and implementation of a VPN deployment. This course will focus your attention on the important criteria that will lead to choosing the right technologies and implementation approach for your particular need.

Who should take this class?

This course is designed to provide in-depth knowledge of VPNs and will benefit anyone who is tasked with implementing a corporate-wide initiative, or anyone who is interested in learning about the technologies available.

What you will learn

What you will learn

- Public versus private networking
- The role of security - cryptography, digital certificates, PKI
- Pros and cons of different VPN Protocols
- Importance of IPSec and protocols that support digital certificates
- Architectural choices for Virtual Private Networking
- Ongoing VPN management

To register online, visit

www.msctrustgate.com/training.htm

MSC Trustgate.com Training Programme

Contact

Tel : 603 8318 1800
Fax : 603 8319 1800

E-mail

Training Enquiry
training@msctrustgate.com

Website

www.msctrustgate.com/training.htm
www.msctrustgate.com

VeriSign AUTHORIZED TRAINING CENTER

msctrustgate.com

TRUSTED INTERNET SERVICES

VeriSign Trust Network

Essential Virtual Private Networks (VPN) Components

Course Outline

Chapter 1: Introduction

- Standard introduction
- Privately owned data networks (pros and cons)
- Public data networks (pros and cons)
- Vulnerabilities
- Secure VPNs
  - Confidentiality
  - Integrity
  - Authentication

Chapter 2: Intro to cryptography and PKI

- Basic cryptography concepts
- Symmetric and asymmetric key cryptography
- PKI and digital signatures

Chapter 3: VPN technologies

- What is a VPN?
- Application layer VPNs
- Network layer VPNs
- Data-link VPNs

Chapter 4: The layer 2 tunneling protocol Concept

- Point to point protocol model
- L2TP model
- Securing L2TP messages
- Why use L2TP?

Chapter 5: IPSec protocol

- IPSec standard and protocols
- Protocol modes
- Authentication header
- Encapsulating security payload
- Security associations
- IPSec key generation, challenges, and specifications

Chapter 6: Key management for IPSecs

- Manual key exchange
- Automated key exchange
- ISAKMP framework
- Internet Key Exchange
- IKE peer authentication

Chapter 7: IKE/IPSec VPNS and PKIs

- Why combine IKE and PKI?
- X.509 digital certificates
- Certificate acquisition and management
- The future of IKE and PKIs

Chapter 8: Designing VPN solutions

- The discovery process
- Identifying goals and objectives
- Understanding requirements
- Designing the right architecture
- Selecting the right technology
- Execution and implementation

Chapter 9: Remote access VPNs

- The big picture
- The real world
- Network architecture
- Client software
- User support

Chapter 10: Remote office VPN implementations

- The big picture
- The real world
- Network architecture

Chapter 11: Intranet VPN implementations

- The big picture
- The real world

Chapter 12: Extranet VPN implementations

- The big picture
- The real world
- User support

Chapter 13: Managing VPNs

- Gateway software management and usage auditing
- Client software
- Authentication
- Authorization

Chapter 14: The future of VPN

- Current and future models for security

MSC Trustgate.com Sdn. Bhd.

Address

Ground Floor, Belatuk Block
Cyberview Garden
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia

Contact

Tel : 603 8318 1800
Fax : 603 8319 1800

Website

www.msctrustgate.com
www.mykeymykad.com.my

REGISTER NOW