

(MTCUME) Certified User Management Engineer

Course Description:

(MTCUME) is a course to understand Mikrotik RouterOS User Management principles. By the end of this training session, the student will be able to securely manage large scale RouterOS based network with centralized user management.

Modes of Trainings Available:

- Online Training
- Class Room Training
- Regular Classes Available
- Weekend Classes Available

Course Outline

PPP

1. PPP

- PPP Profile
- Local and remote addresses
- Incoming and outgoing filters
- Address list
- Change TCP-MSS
- Use encryption
- Session timeout
- Rate-limit configuration
- Only-one setting

2. PPP Secret

- Service and Profile
- Local and Remote address
- Routes configuration
- Limit Bytes In/Limit Bytes Out configuration



3. IP Pool

- Set addresses ranges
- Next pool options

PPTP, L2TP

1. PPTP and L2TP

- Theory
- Comparison

2. PPTP Client configuration

- Client setup
- Set profile
- Dial on demand
- add default route and static routes

3. L2TP Client configuration

- Client setup
- Configure profile
- Dial on demand
- Add default route and static routes

4. L2TP Server configuration

- Enable server
- Set profiles
- Add clients to PPP secret
- Set Static interfaces for clients

PPPoE

1. PPPoE server and client

- Theory
- Usage environment
- Comparison to other PPP protocols

2. PPPoE client configuration

- Client setup
- Select interface
- Service name
- Configure profile



3. PPPoE Server configuration

- Enable PPPoE server
- Set profiles
- Add clients to PPP secret
- Add Static interfaces for clients
- Secure server by removing any IP address from PPPoE server interface

4. Encryption

- Set profile without encryption
- Set profile with encryption
- Configure PPPoE client without encryption

IPsec

1. Introduction

- Theory and concepts
- Comparison to other VPN protocols

2. IPsec Peer

- Use different authentication methods
- IPsec exchange modes
- Encryption and hash algorithms
- NAT-Traversal
- Lifetime and life bytes
- DPD protocol

3. Policy

- IPsec protocol and action
- Tunnels
- Generate dynamic Policy

4. Proposal

- Encryption and authentication algorithms
- Lifetime
- PFS
- Installed-SA
- Flush SA



5. Create IPsec between two routers with NAT

- Set peer
- Set policy
- Set NAT rules
- Confirm the secure link is established

Hotspot

- Introduction
- Concepts
- Usage environments
- Setup Hotspot with default settings

Hotspot Login Methods

- HTTP CHAP/PAP
- MAC
- Cookie
- HTTPS
- Trial
- RADIUS

Users

- Add users
- Set MAC-address for user
- Set MAC-address for username
- Limit Uptime and Limit Bytes In/Out
- Reset limits for user

Monitor Users

- Host Table
- Active Table
- SNMP for users

Profile

- Keepalive timeout
- Shared users
- Rate-Limit
- Address-list
- Incoming/Outgoing filter
- Incoming/Outgoing Packet Mark



Bypass Hotspot

- Walled garden
- Walled garden IP
- IP binding

Customize Hotspot

- Advertisement
- Customize pages

RADIUS

- RADIUS client
- Add radius client
- Set service
- Use RADIUS for the specific service

RADIUS server

- User manager
- Install the latest user-manager
- Add routers
- Add users
- Set profile
- RADIUS incoming

