

1. DNS
2. NTP Client
3. IP ADDRESS
 - Ether2: 192.168.100.1/25
 - Ether3: 192.168.200.1/24
4. DHCP POOL
 - Sebanyak 99 Client
5. FIREWALL
 - Buat IP 192.168.100.2 - 192.168.100.50 tidak bisa ping ke router
 - Buat IP 192.168.100.51 - 192.168.100.100 tidak bisa ping ke client wireless
6. LOG DI DISK
7. ACCOUNT HOTSPOT
 - Buat 20 account hotspot secara random
 - Buat client hanya bisa internetan pada jam 07.00 - 16.00
8. BLOCK Website dan file
 - Block situs linux.org
 - Block file .mp3 dan .mkv
9. PASTIKAN MEMILIKI MIKHMOM KARENA ARSITEKTUR MIKROTIK TIDAK SUPPORT USER MANAGER

- system > reset configuration > no default configuration.

1. DNS

- IP > DHCP Client > New > Ether 1 / Wlan1.
- Jika mau internetan IP > Firewall > NAT > New.
 - Chain: srcnat.
 - Out. Interface: Ether1 / Wlan1.
 - Action: masquerade

2. NTP Client

- System > SNTP Client > Enabled.
 - Primary NTP Server : 0.id.pool.ntp.org.
 - Secondary NTP Server: 1.id.pool.ntp.org.
- Ping Terminal DNS diatas.
- Copy IP yg didapatkan lalu masukkan pada Primary dan Secondary

NTP SERVER.

- Apply.
 - Cek System > Clock (pastikan mendapatkan waktunya Asia/Jakarta).

3. IP Address

- IP > Adresses > New.
 - Ether2: 192.168.100.1/25.
 - Wlan1: 192.168.200.1/24.
 - Ether3: 192.168.200.1/24 (JIKA MENGGUNAKAN TP- Link)

4. DHCP Pool

- IP > DHCP Server > DHCP Setup.
 - Ether2: 192.168.100.2 - 192.168.100.100.
 - Wlan1: 192.168.200.2 -192.168.200.100.
 - Ether3: 192.168.200.2 -192.168.200.100 (JIKA MENGGUNAKAN TP- Link)
 - DNS Server: 8.8.8.8.

5. Firewall

- IP > Firewall > Filter Rules > New.
 - *IP 192.168.100.2 - 192.168.100.50 tidak bisa ping router.*
 - Chain: input.
 - Src. Address: 192.168.100.2 - 192.168.100.50.
 - Protocol: icmp
 - Action: drop.
 - *IP 192.168.100.51 - 192.168.100.100 tidak bisa ping client wireless.*
 - Chain: input.
 - Src. Address: 192.168.100.51 - 192.168.100.100.
 - Dst. Address: 192.168.200.1.
 - Protocol: icmp.
 - Action: drop.

6. LOG Tersimpan di Disk

- IP > Firewall > Filter Rules > New.
 - Chain: input.
 - Action: Log.
 - Log prefix: Tersimpan di Disk.
- System > Logging.
 - Ubah semua Action > disk.

- Dashboard > Log (lihat apakah sudah berubah semuanya menjadi di disk).

7. Account Hotspot

- Wireless > Wifi Interfaces > Wlan1 > Enable.
- Wireless.
 - Mode: ap bridge.
 - Band: 2GHz-B/G/N
 - SSID: Andrean@ProxyUkk.
- Apply.
- IP > Hotspot > Hotspot Setup > Wlan1 / Ether3.
 - DNS Servers: 8.8.8.8
 - DNS Name: Andrean.net
 - Name = Password User: admin.
 - Server Profiles > hsprof1
 - Matikan cookie dan centang RADIUS
- System > Users > Groups > New.
 - Name: mikhmon.
 - Policies: write, api, read, sensitive.
 - Apply.
- Users > New.
 - Name: mikhmon.
 - Group: mikhmon.
 - Password: 1234.
 - Confirm Password: 1234.

8. Jalankan MAMP > Jalankan WebServer > Apache

- Open browser: localhost:8888/mikhmon/mikhmon.
 - Username: mikhmon
 - Password: 1234
- Add router.
 - Session name: Andrean (bebas)
 - IP Mikrotik: 192.168.200.1
 - Username: mikhmon
 - Password: 1234
 - Hotspot name: Andrean@ProxyUKK
 - DNS Name: Andrean.net
- Connect.
- User Profile > Add.
 - Name: 20 ORANG

- Users > Generate.
 - Qty: 20
 - Usermode: username=password
 - Name length: 4
 - Profile: 20 ORANG
 - Characters: bebas mau pilih apa aja
- Generate.

9. Membuat client wireless hanya bisa internetan pada jam 07:00 - 16:00

- IP > Firewall > Nat > Cari yang Chain srcnat, Action masquerade, dan Out. Interface ether1.
 - Tab Extra > Time 07:00:00 - 16:00:00

10. Blokir Website

- IP > Firewall > Filter Rules > New
 - Chain: forward
 - Advanced > Content: linux.org
 - Action > drop
- Selanjutnya ping di terminal Mac OS > nslookup linux.org
- Copy semua IP nya lalu..
 - Chain: forward
 - Dst. Address: masukan IP yang tadi dicari.
 - Action > drop

12. Blokir File

- IP > Firewall > Filter Rules > New
 - Chain: forward
 - Advanced > Content: .mp3
 - Action > drop
- IP > Firewall > Filter Rules > New
 - Chain: forward
 - Advanced > Content: .mkv
 - Action > drop