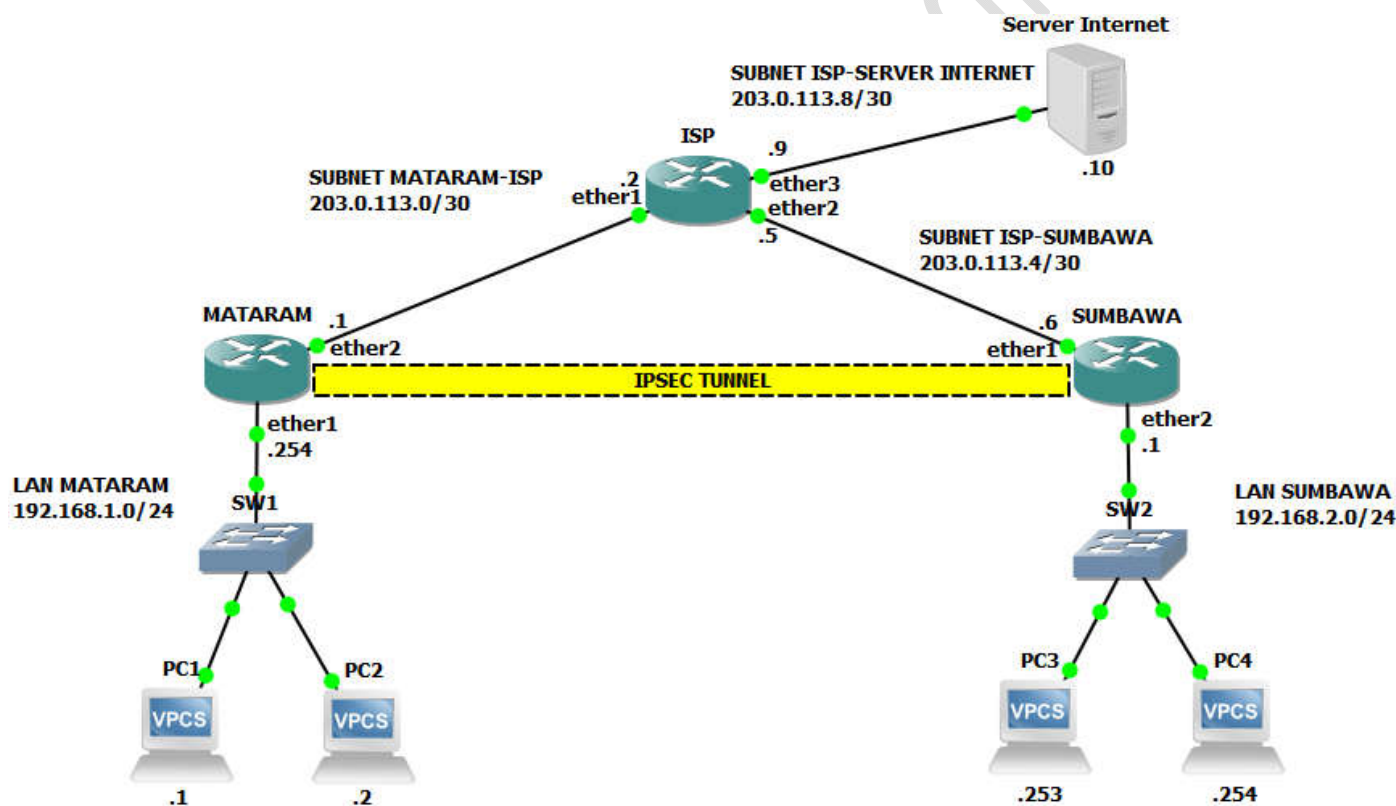


## KONFIGURASI SITE-TO-SITE IPSEC VPN TUNNEL DI MIKROTIK MENGGUNAKAN GNS3

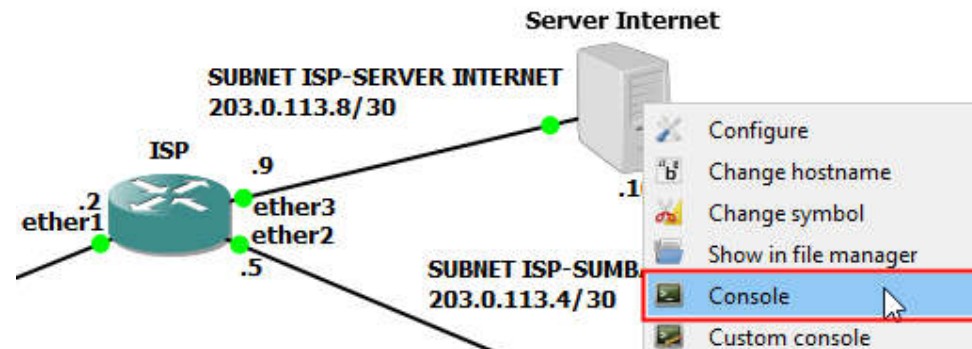
Oleh I Putu Hariyadi [ [admin@iputuhariyadi.net](mailto:admin@iputuhariyadi.net) ]

### A. TOPOLOGI JARINGAN



## B. KONFIGURASI PENGALAMATAN IP DAN VERIFIKASI KONEKSI DI VPCS SERVER INTERNET

Pengaturan pengalamatan IP dapat dilakukan dengan cara klik kanan pada *VPCS Server Internet* dan pilih *Console*, seperti terlihat pada gambar berikut:



Tampil kotak dialog *Virtual PC Simulator Server Internet*. Untuk mengatur pengalamatan IP dan *default gateway* digunakan perintah **ip alamat-ip/subnetmask default-gateway**, seperti terlihat pada gambar berikut:

```

Server Internet
VPCS> ip 203.0.113.10/30 203.0.113.9
Checking for duplicate address...
PC1 : 203.0.113.10 255.255.255.252 gateway 203.0.113.9
  
```

Sedangkan perintah **show ip** digunakan untuk menampilkan informasi pengalamatan IP yang telah diatur, seperti terlihat pada gambar berikut:

```
VPCS> show ip

NAME       : VPCS[1]
IP/MASK     : 203.0.113.10/30
GATEWAY     : 203.0.113.9
DNS         :
MAC        : 00:50:79:66:68:04
LPORT      : 10017
RHOST:PORT  : 127.0.0.1:10016
MTU         : 1500
```

### C. KONFIGURASI DI ROUTER ISP

Adapun langkah-langkah konfigurasi yang dilakukan di *router ISP* adalah sebagai berikut:

1. Mengatur *hostname*.

```
[admin@MikroTik] > system identity set name=ISP
```

2. Mengatur pengalamatan IP pada *interface ether1*.

```
[admin@ISP] > ip address add address=203.0.113.2/30 interface=ether1
```

3. Mengatur pengalamatan IP pada *interface ether2*.

```
[admin@ISP] > ip address add address=203.0.113.5/30 interface=ether2
```

4. Mengatur pengalamatan IP pada *interface ether3*.

```
[admin@ISP] > ip address add address=203.0.113.9/30 interface=ether3
```

5. Menampilkan informasi pengalamatan IP pada *interface*.

```
[admin@ISP] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#  ADDRESS      NETWORK      INTERFACE
0  203.0.113.2/30  203.0.113.0  ether1
1  203.0.113.5/30  203.0.113.4  ether2
2  203.0.113.9/30  203.0.113.8  ether3
```

- Memverifikasi koneksi ke *Server Internet*.

```
[admin@ISP] > ping 203.0.113.10
```

| SEQ | HOST         | SIZE | TTL | TIME | STATUS |
|-----|--------------|------|-----|------|--------|
| 0   | 203.0.113.10 | 56   | 64  | 26ms |        |
| 1   | 203.0.113.10 | 56   | 64  | 16ms |        |
| 2   | 203.0.113.10 | 56   | 64  | 47ms |        |

```
sent=3 received=3 packet-loss=0% min-rtt=16ms avg-rtt=29ms max-rtt=47ms
```

Terlihat koneksi telah berhasil dilakukan.

#### D. KONFIGURASI DASAR DI ROUTER MATARAM

Adapun langkah-langkah konfigurasi dasar yang dilakukan di *router MATARAM* adalah sebagai berikut:

- Mengatur *hostname*.

```
[admin@MikroTik] > system identity set name=MATARAM
```

- Menampilkan informasi keseluruhan *interface*.

```
[admin@MATARAM] > interface print
```

Flags: D - dynamic, X - disabled, R - running, S - slave

| # | NAME     | TYPE  | ACTUAL-MTU | L2MTU | MAX-L2MTU | MAC-ADDRESS       |
|---|----------|-------|------------|-------|-----------|-------------------|
| 0 | R ether1 | ether | 1500       |       |           | 00:00:AB:90:11:00 |
| 1 | R ether2 | ether | 1500       |       |           | 00:00:AB:90:11:01 |
| 2 | R ether3 | ether | 1500       |       |           | 00:00:AB:90:11:02 |
| 3 | R ether4 | ether | 1500       |       |           | 00:00:AB:90:11:03 |
| 4 | R ether5 | ether | 1500       |       |           | 00:00:AB:90:11:04 |

- Mengubah nama *interface ether1* menjadi *local*.

```
[admin@MATARAM] > interface set ether1 name=local
```

- Mengubah nama *interface ether2* menjadi *public*.

```
[admin@MATARAM] > interface set ether2 name=public
```

5. Memverifikasi perubahan nama *interface*.

```
[admin@MATARAM] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#      NAME      TYPE      ACTUAL-MTU  L2MTU  MAX-L2MTU  MAC-ADDRESS
0  R  ether3      ether      1500      1500      1500      00:00:AB:90:11:02
1  R  ether4      ether      1500      1500      1500      00:00:AB:90:11:03
2  R  ether5      ether      1500      1500      1500      00:00:AB:90:11:04
3  R  local       ether      1500      1500      1500      00:00:AB:90:11:00
4  R  public      ether      1500      1500      1500      00:00:AB:90:11:01
```

6. Mengatur pengalamatan IP pada *interface public*.

```
[admin@MATARAM] > ip address add address=203.0.113.1/30 interface=public
```

7. Mengatur pengalamatan IP pada *interface local*.

```
[admin@MATARAM] > ip address add address=192.168.1.254/24 interface=local
```

8. Menampilkan informasi pengalamatan IP pada *interface*.

```
[admin@MATARAM] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#      ADDRESS      NETWORK      INTERFACE
0  203.0.113.1/30    203.0.113.0    public
1  192.168.1.254/24  192.168.1.0    local
```

9. Menampilkan informasi tabel *routing*.

```
[admin@MATARAM] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf,
m - mme,
B - blackhole, U - unreachable, P - prohibit
#      DST-ADDRESS      PREF-SRC      GATEWAY      DISTANCE
0  ADC  192.168.1.0/24    192.168.1.254  local        0
1  ADC  203.0.113.0/30    203.0.113.1    public        0
```

10. Mengatur *default route* ke *router ISP*.

```
[admin@MATARAM] > ip route add gateway=203.0.113.2
```

11. Menampilkan informasi tabel *routing*.

```
[admin@MATARAM] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf,
m - mme,
B - blackhole, U - unreachable, P - prohibit
#      DST-ADDRESS      PREF-SRC      GATEWAY      DISTANCE
0 A S   0.0.0.0/0           203.0.113.2      1
1 ADC   192.168.1.0/24      192.168.1.254    local         0
2 ADC   203.0.113.0/30     203.0.113.1      public        0
```

12. Mengatur *Internet Connection Sharing (ICS)* menggunakan *IP Firewall NAT* agar *client* di LAN Mataram dapat terkoneksi ke *ISP* dan dapat mengakses *Server Internet*.

```
[admin@MATARAM] > ip firewall nat add chain=srcnat out-interface=public action=masquerade
```

13. Memverifikasi pengaturan *IP Firewall NAT*.

```
[admin@MATARAM] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
0      chain=srcnat action=masquerade out-interface=public
```

14. Memverifikasi koneksi ke *ISP*.

```
[admin@MATARAM] > ping 203.0.113.2
SEQ HOST                                     SIZE TTL TIME   STATUS
0 203.0.113.2                               56  64 43ms
1 203.0.113.2                               56  64 25ms
2 203.0.113.2                               56  64 56ms
sent=3 received=3 packet-loss=0% min-rtt=25ms avg-rtt=41ms max-rtt=56ms
```

Terlihat koneksi telah berhasil dilakukan.

15. Memverifikasi koneksi ke *Server Internet*.

```
[admin@MATARAM] > ping 203.0.113.10
```

| SEQ | HOST         | SIZE | TTL | TIME | STATUS |
|-----|--------------|------|-----|------|--------|
| 0   | 203.0.113.10 | 56   | 63  | 38ms |        |
| 1   | 203.0.113.10 | 56   | 63  | 25ms |        |
| 2   | 203.0.113.10 | 56   | 63  | 68ms |        |

sent=3 received=3 packet-loss=0% min-rtt=25ms avg-rtt=43ms max-rtt=68ms

Terlihat koneksi telah berhasil dilakukan.

16. Memverifikasi rute yang dilalui oleh paket dari router MATARAM ke Server Internet menggunakan *traceroute*.

```
[admin@MATARAM] > tool traceroute 203.0.113.10
```

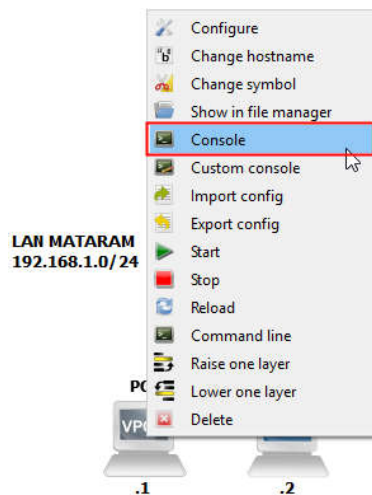
| # | ADDRESS      | LOSS | SENT | LAST   | AVG  | BEST | WORST | STD-DEV | STATUS |
|---|--------------|------|------|--------|------|------|-------|---------|--------|
| 1 | 203.0.113.2  | 0%   | 7    | 19ms   | 41.2 | 7.3  | 140.7 | 42.3    |        |
| 2 | 203.0.113.10 | 0%   | 7    | 28.7ms | 31.7 | 20.2 | 58.3  | 11.6    |        |

Berdasarkan *output* dari eksekusi perintah *traceroute*, terlihat rute perjalanan paket dari *router MATARAM* ke *Server Internet* adalah melalui *router ISP* (203.0.113.2).

## E. KONFIGURASI PENGALAMATAN IP DAN VERIFIKASI KONEKSI DI VPCS PC1

Adapun langkah-langkah konfigurasi pengalamatan IP dan verifikasi koneksi di VPCS PC1 adalah sebagai berikut:

1. Pengaturan pengalamatan IP dapat dilakukan dengan cara klik kanan pada *VPCS PC1* dan pilih *Console*, seperti terlihat pada gambar berikut:



Tampil kotak dialog *Virtual PC Simulator PC1*. Untuk mengatur pengalamatan IP dan *default gateway* digunakan perintah **ip alamat-ip/subnetmask default-gateway**, seperti terlihat pada gambar berikut:

```
PC1> ip 192.168.1.1/24 192.168.1.254
Checking for duplicate address...
PC1 : 192.168.1.1 255.255.255.0 gateway 192.168.1.254
```

2. Menampilkan informasi pengalamatan IP yang telah diatur menggunakan perintah **show ip**, seperti terlihat pada gambar berikut:



```
PC1> show ip  
NAME       : PC1[1]  
IP/MASK    : 192.168.1.1/24  
GATEWAY    : 192.168.1.254  
DNS        :  
MAC        : 00:50:79:66:68:00  
LPORT      : 10010  
RHOST:PORT : 127.0.0.1:10011  
MTU        : 1500
```

3. Memverifikasi koneksi ke *router MATARAM* yang berfungsi sebagai *gateway*.

```
PC1> ping 192.168.1.254  
84 bytes from 192.168.1.254 icmp_seq=1 ttl=64 time=9.005 ms  
84 bytes from 192.168.1.254 icmp_seq=2 ttl=64 time=27.014 ms  
84 bytes from 192.168.1.254 icmp_seq=3 ttl=64 time=15.009 ms  
84 bytes from 192.168.1.254 icmp_seq=4 ttl=64 time=6.002 ms  
84 bytes from 192.168.1.254 icmp_seq=5 ttl=64 time=7.000 ms
```

Koneksi berhasil dilakukan.

4. Memverifikasi koneksi ke *ISP*.

```
PC1> ping 203.0.113.2  
84 bytes from 203.0.113.2 icmp_seq=1 ttl=63 time=71.045 ms  
84 bytes from 203.0.113.2 icmp_seq=2 ttl=63 time=33.021 ms  
84 bytes from 203.0.113.2 icmp_seq=3 ttl=63 time=36.019 ms  
84 bytes from 203.0.113.2 icmp_seq=4 ttl=63 time=48.026 ms  
84 bytes from 203.0.113.2 icmp_seq=5 ttl=63 time=81.050 ms
```

Koneksi berhasil dilakukan.

5. Memverifikasi koneksi ke *Server Internet*.

```
PC1> ping 203.0.113.10
84 bytes from 203.0.113.10 icmp_seq=1 ttl=62 time=65.039 ms
84 bytes from 203.0.113.10 icmp_seq=2 ttl=62 time=53.038 ms
84 bytes from 203.0.113.10 icmp_seq=3 ttl=62 time=38.021 ms
84 bytes from 203.0.113.10 icmp_seq=4 ttl=62 time=74.043 ms
84 bytes from 203.0.113.10 icmp_seq=5 ttl=62 time=90.047 ms
```

Koneksi berhasil dilakukan.

- Memverifikasi rute yang dilalui oleh paket dari *PC1* ke *Server Internet* menggunakan perintah *trace*.

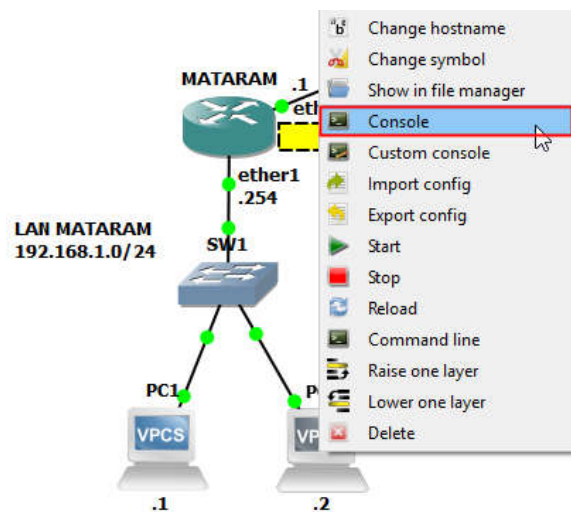
```
PC1> trace 203.0.113.10
trace to 203.0.113.10, 8 hops max, press Ctrl+C to stop
 1  192.168.1.254    35.023 ms  31.020 ms  12.007 ms
 2  203.0.113.2     58.039 ms  53.033 ms  43.028 ms
 3  *203.0.113.10   56.036 ms (ICMP type:3, code:3, Destination port unreachable)
```

Berdasarkan *output* dari eksekusi perintah *trace*, terlihat rute perjalanan paket dari *PC1* ke *Server Internet* adalah melalui *router MATARAM* (192.168.1.254) → *router ISP* (203.0.113.2).

## F. KONFIGURASI PENGALAMATAN IP DAN VERIFIKASI KONEKSI DI VPCS PC2

Adapun langkah-langkah konfigurasi pengalamatan IP dan verifikasi koneksi di VPCS PC2 adalah sebagai berikut:

- Pengaturan pengalamatan IP dapat dilakukan dengan cara klik kanan pada *VPCS PC2* dan pilih *Console*, seperti terlihat pada gambar berikut:



Tampil kotak dialog *Virtual PC Simulator PC2*. Untuk mengatur pengalamatan IP dan *default gateway* digunakan perintah **ip alamat-subnetmask default-gateway**, seperti terlihat pada gambar berikut:

```
PC2> ip 192.168.1.2/24 192.168.1.254
Checking for duplicate address...
PC1 : 192.168.1.2 255.255.255.0 gateway 192.168.1.254
```

- Menampilkan informasi pengalamatan IP yang telah diatur menggunakan perintah **show ip**, seperti terlihat pada gambar berikut:

```
PC2> show ip

NAME       : PC2[1]
IP/MASK     : 192.168.1.2/24
GATEWAY     : 192.168.1.254
DNS         :
MAC        : 00:50:79:66:68:01
LPORT      : 10012
RHOST:PORT  : 127.0.0.1:10013
MTU         : 1500
```

3. Memverifikasi koneksi ke *router MATARAM* yang berfungsi sebagai *gateway*.

```
PC2> ping 192.168.1.254
84 bytes from 192.168.1.254 icmp_seq=1 ttl=64 time=20.011 ms
84 bytes from 192.168.1.254 icmp_seq=2 ttl=64 time=9.006 ms
84 bytes from 192.168.1.254 icmp_seq=3 ttl=64 time=22.010 ms
84 bytes from 192.168.1.254 icmp_seq=4 ttl=64 time=13.004 ms
84 bytes from 192.168.1.254 icmp_seq=5 ttl=64 time=10.010 ms
```

Koneksi berhasil dilakukan.

4. Memverifikasi koneksi ke *ISP*.

```
PC2> ping 203.0.113.2
84 bytes from 203.0.113.2 icmp_seq=1 ttl=63 time=27.014 ms
84 bytes from 203.0.113.2 icmp_seq=2 ttl=63 time=23.010 ms
84 bytes from 203.0.113.2 icmp_seq=3 ttl=63 time=21.011 ms
84 bytes from 203.0.113.2 icmp_seq=4 ttl=63 time=53.032 ms
84 bytes from 203.0.113.2 icmp_seq=5 ttl=63 time=74.047 ms
```

Koneksi berhasil dilakukan.

5. Memverifikasi koneksi ke *Server Internet*.

```
PC2> ping 203.0.113.10
84 bytes from 203.0.113.10 icmp_seq=1 ttl=62 time=46.026 ms
84 bytes from 203.0.113.10 icmp_seq=2 ttl=62 time=90.057 ms
84 bytes from 203.0.113.10 icmp_seq=3 ttl=62 time=47.029 ms
84 bytes from 203.0.113.10 icmp_seq=4 ttl=62 time=34.020 ms
84 bytes from 203.0.113.10 icmp_seq=5 ttl=62 time=52.029 ms
```

Koneksi berhasil dilakukan.

- Memverifikasi rute yang dilalui oleh paket dari *PC2* ke *Server Internet* menggunakan perintah *trace*.

```
PC2> trace 203.0.113.10
trace to 203.0.113.10, 8 hops max, press Ctrl+C to stop
 1  192.168.1.254    30.021 ms  26.017 ms  11.002 ms
 2  203.0.113.2     35.019 ms  30.018 ms  40.025 ms
 3  *203.0.113.10   48.030 ms (ICMP type:3, code:3, Destination port unreachable)
```

Berdasarkan *output* dari eksekusi perintah *trace*, terlihat rute perjalanan paket dari *PC2* ke *Server Internet* adalah melalui *router MATARAM* (192.168.1.254) → *router ISP* (203.0.113.2).

## G. KONFIGURASI DASAR DI ROUTER SUMBAWA

Adapun langkah-langkah konfigurasi dasar yang dilakukan di *router SUMBAWA* adalah sebagai berikut:

- Mengatur *hostname*.

```
[admin@MikroTik] > system identity set name=SUMBAWA
```

- Menampilkan informasi keseluruhan *interface*.

```
[admin@SUMBAWA] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#      NAME      TYPE      ACTUAL-MTU  L2MTU  MAX-L2MTU  MAC-ADDRESS
0  R  ether1      ether      1500      1500      1500      00:00:AB:14:E7:00
1  R  ether2      ether      1500      1500      1500      00:00:AB:14:E7:01
2  R  ether3      ether      1500      1500      1500      00:00:AB:14:E7:02
3  R  ether4      ether      1500      1500      1500      00:00:AB:14:E7:03
4  R  ether5      ether      1500      1500      1500      00:00:AB:14:E7:04
```

3. Mengubah nama *interface ether1* menjadi *public*.

```
[admin@SUMBAWA] > interface set ether1 name=public
```

4. Mengubah nama *interface ether2* menjadi *local*.

```
[admin@SUMBAWA] > interface set ether2 name=local
```

5. Memverifikasi perubahan nama *interface*.

```
[admin@SUMBAWA] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#      NAME      TYPE      ACTUAL-MTU  L2MTU  MAX-L2MTU  MAC-ADDRESS
0  R  ether3      ether      1500      1500      1500      00:00:AB:14:E7:02
1  R  ether4      ether      1500      1500      1500      00:00:AB:14:E7:03
2  R  ether5      ether      1500      1500      1500      00:00:AB:14:E7:04
3  R  local       ether      1500      1500      1500      00:00:AB:14:E7:01
4  R  public      ether      1500      1500      1500      00:00:AB:14:E7:00
```

6. Mengatur pengalamatan IP pada *interface public*.

```
[admin@SUMBAWA] > ip address add address=203.0.113.6/30 interface=public
```

7. Mengatur pengalamatan IP pada *interface local*.

```
[admin@SUMBAWA] > ip address add address=192.168.2.1/24 interface=local
```

8. Menampilkan informasi pengalamatan IP pada *interface*.

```
[admin@SUMBAWA] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS          NETWORK          INTERFACE
0   203.0.113.6/30    203.0.113.4     public
1   192.168.2.1/24    192.168.2.0     local
```

9. Menampilkan informasi tabel *routing*.

```
[admin@SUMBAWA] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf,
m - mme,
B - blackhole, U - unreachable, P - prohibit
#   DST-ADDRESS      PREF-SRC        GATEWAY          DISTANCE
0 ADC 192.168.2.0/24    192.168.2.1     local            0
1 ADC 203.0.113.4/30   203.0.113.6     public           0
```

10. Mengatur *default route* ke router ISP.

```
[admin@SUMBAWA] > ip route add gateway=203.0.113.5
```

11. Menampilkan informasi tabel *routing*.

```
[admin@SUMBAWA] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf,
m - mme,
B - blackhole, U - unreachable, P - prohibit
#   DST-ADDRESS      PREF-SRC        GATEWAY          DISTANCE
0 A S 0.0.0.0/0        203.0.113.5     1
1 ADC 192.168.2.0/24    192.168.2.1     local            0
2 ADC 203.0.113.4/30   203.0.113.6     public           0
```

12. Mengatur *Internet Connection Sharing (ICS)* menggunakan IP Firewall NAT agar *client* di LAN Sumbawa dapat terkoneksi ke *ISP* dan dapat mengakses *Server Internet*.

```
[admin@SUMBAWA] > ip firewall nat add chain=srcnat out-interface=public action=masquerade
```

13. Memverifikasikan pengaturan *IP Firewall NAT*.

```
[admin@SUMBAWA] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
0      chain=srcnat action=masquerade out-interface=public
```

14. Memverifikasi koneksi ke *ISP*.

```
[admin@SUMBAWA] > ping 203.0.113.5
SEQ HOST                                SIZE TTL TIME   STATUS
0 203.0.113.5                          56  64 52ms
1 203.0.113.5                          56  64 47ms
2 203.0.113.5                          56  64 22ms
sent=3 received=3 packet-loss=0% min-rtt=22ms avg-rtt=40ms max-rtt=52ms
```

Terlihat koneksi telah berhasil dilakukan.

15. Memverifikasi koneksi ke *Server Internet*.

```
[admin@SUMBAWA] > ping 203.0.113.10
SEQ HOST                                SIZE TTL TIME   STATUS
0 203.0.113.10                          56  63 52ms
1 203.0.113.10                          56  63 66ms
2 203.0.113.10                          56  63 54ms
sent=3 received=3 packet-loss=0% min-rtt=52ms avg-rtt=57ms max-rtt=66ms
```

Terlihat koneksi telah berhasil dilakukan.

16. Memverifikasi rute yang dilalui oleh paket dari *router SUMBAWA* ke *Server Internet* menggunakan *traceroute*.

```
[admin@SUMBAWA] > tool traceroute 203.0.113.10
```



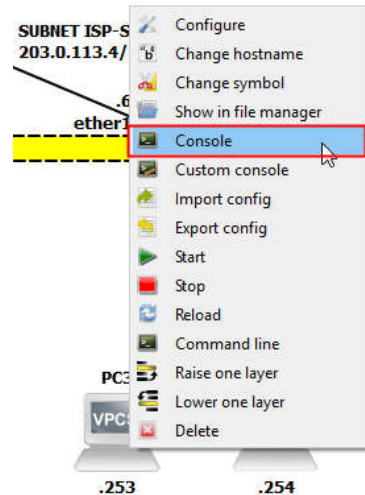
| # | ADDRESS      | LOSS | SENT | LAST   | AVG  | BEST | WORST | STD-DEV | STATUS |
|---|--------------|------|------|--------|------|------|-------|---------|--------|
| 1 | 203.0.113.5  | 0%   | 4    | 18.6ms | 38.7 | 18.6 | 56.1  | 14.2    |        |
| 2 | 203.0.113.10 | 0%   | 4    | 27.7ms | 42.3 | 27.7 | 69    | 15.8    |        |

Berdasarkan *output* dari eksekusi perintah *traceroute*, terlihat rute perjalanan paket dari *router SUMBAWA* ke *Server Internet* adalah melalui *router ISP* (203.0.113.5).

#### H. KONFIGURASI PENGALAMATAN IP DAN VERIFIKASI KONEKSI DI VPCS PC3

Adapun langkah-langkah konfigurasi pengalamatan IP dan verifikasi koneksi di *VPCS PC3* adalah sebagai berikut:

1. Pengaturan pengalamatan IP dapat dilakukan dengan cara klik kanan pada *VPCS PC3* dan pilih *Console*, seperti terlihat pada gambar berikut:



Tampil kotak dialog *Virtual PC Simulator PC3*. Untuk mengatur pengalamatan IP dan *default gateway* digunakan perintah **ip alamat-ip/subnetmask default-gateway**, seperti terlihat pada gambar berikut:

```
PC3> ip 192.168.2.253/24 192.168.2.1
Checking for duplicate address...
PC1 : 192.168.2.253 255.255.255.0 gateway 192.168.2.1
```

2. Menampilkan informasi pengalamatan IP yang telah diatur menggunakan perintah **show ip**, seperti terlihat pada gambar berikut:

```
PC3> show ip

NAME       : PC3[1]
IP/MASK     : 192.168.2.253/24
GATEWAY     : 192.168.2.1
DNS         :
MAC         : 00:50:79:66:68:02
LPORT      : 10006
RHOST:PORT  : 127.0.0.1:10007
MTU         : 1500
```

3. Memverifikasi koneksi ke *router SUMBAWA* yang berfungsi sebagai *gateway*.

```
PC3> ping 192.168.2.1
84 bytes from 192.168.2.1 icmp_seq=1 ttl=64 time=25.015 ms
84 bytes from 192.168.2.1 icmp_seq=2 ttl=64 time=12.006 ms
84 bytes from 192.168.2.1 icmp_seq=3 ttl=64 time=17.007 ms
84 bytes from 192.168.2.1 icmp_seq=4 ttl=64 time=30.021 ms
84 bytes from 192.168.2.1 icmp_seq=5 ttl=64 time=16.011 ms
```

Koneksi berhasil dilakukan.

4. Memverifikasi koneksi ke *ISP*.

```
PC3> ping 203.0.113.5
84 bytes from 203.0.113.5 icmp_seq=1 ttl=63 time=52.030 ms
84 bytes from 203.0.113.5 icmp_seq=2 ttl=63 time=79.054 ms
84 bytes from 203.0.113.5 icmp_seq=3 ttl=63 time=84.056 ms
84 bytes from 203.0.113.5 icmp_seq=4 ttl=63 time=65.045 ms
84 bytes from 203.0.113.5 icmp_seq=5 ttl=63 time=84.053 ms
```

Koneksi berhasil dilakukan.

5. Memverifikasi koneksi ke *Server Internet*.

```
PC3> ping 203.0.113.10
84 bytes from 203.0.113.10 icmp_seq=1 ttl=62 time=85.057 ms
84 bytes from 203.0.113.10 icmp_seq=2 ttl=62 time=42.028 ms
84 bytes from 203.0.113.10 icmp_seq=3 ttl=62 time=63.041 ms
84 bytes from 203.0.113.10 icmp_seq=4 ttl=62 time=41.024 ms
84 bytes from 203.0.113.10 icmp_seq=5 ttl=62 time=78.053 ms
```

Koneksi berhasil dilakukan.

6. Memverifikasi rute yang dilalui oleh paket dari *PC3* ke *Server Internet* menggunakan perintah *trace*.

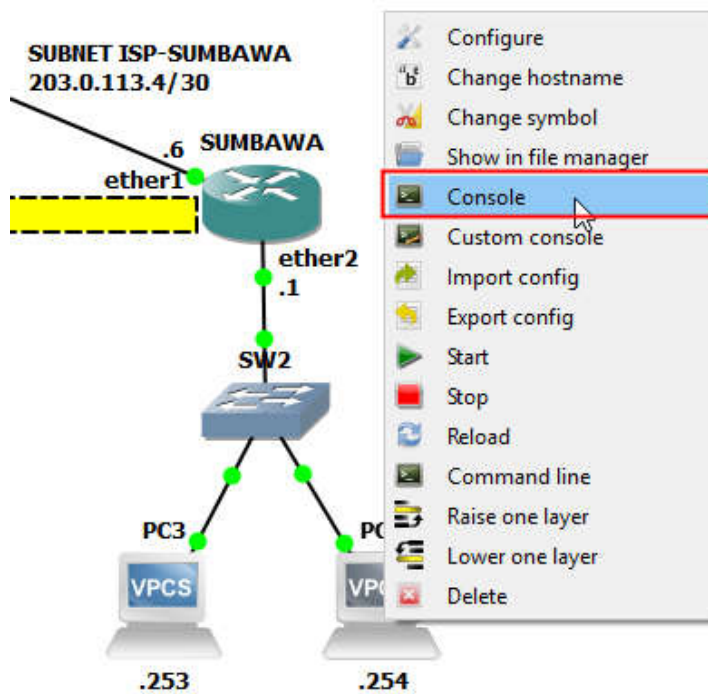
```
PC3> trace 203.0.113.10
trace to 203.0.113.10, 8 hops max, press Ctrl+C to stop
 1  192.168.2.1    19.978 ms  7.006 ms  4.995 ms
 2  203.0.113.5   73.049 ms 35.021 ms 29.018 ms
 3  *203.0.113.10 53.032 ms (ICMP type:3, code:3, Destination port unreachable)
```

Berdasarkan *output* dari eksekusi perintah *trace*, terlihat rute perjalanan paket dari *PC3* ke *Server Internet* adalah melalui *router SUMBAWA* (192.168.2.1) → *router ISP* (203.0.113.5).

## I. KONFIGURASI PENGALAMATAN IP DAN VERIFIKASI KONEKSI DI VPCS PC4

Adapun langkah-langkah konfigurasi pengalamatan IP dan verifikasi koneksi di *VPCS PC4* adalah sebagai berikut:

1. Pengaturan pengalamatan IP dapat dilakukan dengan cara klik kanan pada *VPCS PC4* dan pilih *Console*, seperti terlihat pada gambar berikut:



Tampil kotak dialog *Virtual PC Simulator PC4*. Untuk mengatur pengalamatan IP dan *default gateway* digunakan perintah **ip alamat-ip/subnetmask default-gateway**, seperti terlihat pada gambar berikut:

```
PC4> ip 192.168.2.254/24 192.168.2.1
Checking for duplicate address...
PC1 : 192.168.2.254 255.255.255.0 gateway 192.168.2.1
```

2. Menampilkan informasi pengalamatan IP yang telah diatur menggunakan perintah **show ip**, seperti terlihat pada gambar berikut:

```
PC4> show ip
NAME       : PC4[1]
IP/MASK    : 192.168.2.254/24
GATEWAY    : 192.168.2.1
DNS        :
MAC        : 00:50:79:66:68:03
LPORT     : 10008
RHOST:PORT : 127.0.0.1:10009
MTU        : 1500
```

3. Memverifikasi koneksi ke *router SUMBAWA* yang berfungsi sebagai *gateway*.

```
PC4> ping 192.168.2.1
84 bytes from 192.168.2.1 icmp_seq=1 ttl=64 time=28.017 ms
84 bytes from 192.168.2.1 icmp_seq=2 ttl=64 time=7.001 ms
84 bytes from 192.168.2.1 icmp_seq=3 ttl=64 time=5.002 ms
84 bytes from 192.168.2.1 icmp_seq=4 ttl=64 time=12.005 ms
84 bytes from 192.168.2.1 icmp_seq=5 ttl=64 time=9.003 ms
```

Koneksi berhasil dilakukan.

4. Memverifikasi koneksi ke *ISP*.

```
PC4> ping 203.0.113.5
84 bytes from 203.0.113.5 icmp_seq=1 ttl=63 time=41.024 ms
84 bytes from 203.0.113.5 icmp_seq=2 ttl=63 time=67.043 ms
84 bytes from 203.0.113.5 icmp_seq=3 ttl=63 time=53.032 ms
84 bytes from 203.0.113.5 icmp_seq=4 ttl=63 time=27.002 ms
84 bytes from 203.0.113.5 icmp_seq=5 ttl=63 time=81.053 ms
```

Koneksi berhasil dilakukan.

5. Memverifikasi koneksi ke *Server Internet*.

```
PC4> ping 203.0.113.10
84 bytes from 203.0.113.10 icmp_seq=1 ttl=62 time=46.034 ms
84 bytes from 203.0.113.10 icmp_seq=2 ttl=62 time=70.044 ms
84 bytes from 203.0.113.10 icmp_seq=3 ttl=62 time=49.027 ms
84 bytes from 203.0.113.10 icmp_seq=4 ttl=62 time=89.054 ms
84 bytes from 203.0.113.10 icmp_seq=5 ttl=62 time=47.029 ms
```

Koneksi berhasil dilakukan.

- Memverifikasi rute yang dilalui oleh paket dari *PC4* ke *Server Internet* menggunakan perintah *trace*.

```
PC4> trace 203.0.113.10
trace to 203.0.113.10, 8 hops max, press Ctrl+C to stop
 1  192.168.2.1    16.009 ms  13.008 ms  5.001 ms
 2  203.0.113.5    51.028 ms  36.022 ms  30.020 ms
 3  *203.0.113.10  44.028 ms (ICMP type:3, code:3, Destination port unreachable)
```

Berdasarkan *output* dari eksekusi perintah *trace*, terlihat rute perjalanan paket dari *PC4* ke *Server Internet* adalah melalui *router SUMBAWA* (192.168.2.1) → *router ISP* (203.0.113.5).

## J. KONFIGURASI IPSEC DI ROUTER MATARAM

Adapun langkah-langkah konfigurasi *IPSEC VPN Tunnel* di *router MATARAM* adalah sebagai berikut:

- Melakukan pengaturan *IPSec Peer* dengan *router SUMBAWA*. *IPSec Peer* digunakan untuk membentuk koneksi antara *Internet Key Exchange (IKE) daemon* yaitu pada konfigurasi *phase 1*. Koneksi yang telah terbentuk ini akan digunakan untuk negosiasi *keys* dan algoritma untuk *Security Association (SA)*.

```
[admin@MATARAM] > ip ipsec peer add address=203.0.113.6 port=500 auth-method=pre-shared-key secret=12345678
```

Penjelasan parameter:

- a) **address**, digunakan untuk menentukan alamat IP dari *remote peer* yaitu 203.0.113.6 yang merupakan alamat IP dari *router SUMBAWA*.
- b) **port**, digunakan untuk menentukan nomor *port* komunikasi ke *remote peer* yaitu 500.
- c) **auth-method**, digunakan untuk menentukan metode otentikasi yaitu *pre-shared-key* yang merupakan metode otentikasi menggunakan sandi yang telah dibagi pakai antar *peer*.
- d) **secret**, digunakan untuk mengatur sandi ketika metode otentikasi yang digunakan adalah *pre-shared-key* yaitu 12345678.

2. Memverifikasi pengaturan *IPSec Peer*.

```
[admin@MATARAM] > ip ipsec peer print
Flags: X - disabled, D - dynamic
0   address=203.0.113.6/32 local-address=:: passive=no port=500 auth-method=pre-shared-key
    secret="12345678" generate-policy=no policy-template-group=default exchange-mode=main
    send-initial-contact=yes nat-traversal=yes proposal-check=obey hash-algorithm=sha1
    enc-algorithm=aes-128,3des dh-group=modp1024 lifetime=1d lifeytes=0 dpd-interval=2m
    dpd-maximum-failures=5
```

3. Mengatur *IPSec Proposal* untuk menentukan algoritma otentikasi dan enkripsi yang digunakan oleh router. Informasi *proposal* akan dikirimkan oleh *IKE daemon* untuk membentuk *Security Association (SA)* dari *IPSec Policy* pada *phase 2*. Kedua router yaitu *MATARAM* dan *SUMBAWA* harus menggunakan algoritma yang sama. Mikrotik telah membuatkan satu *IPSec Proposal* dengan nama “**default**” yang menggunakan algoritma otentikasi “**sha1**” dan algoritma enkripsi “**aes-256-cbc,aes-192-cbc,aes-128-cbc**” dimana masing-masing ditunjukkan pada parameter *auth-algorithms* dan *enc-algorithms*.

```
[admin@MATARAM] > ip ipsec proposal print
Flags: X - disabled, * - default
0   * name="default" auth-algorithms=sha1 enc-algorithms=aes-256-cbc,aes-192-cbc,aes-128-cbc lifetime=30m
    pfs-group=modp1024
```

Studi kasus konfigurasi *Site-to-Site IPSec VPN Tunnel* ini menggunakan proposal “*default*”.

4. Mengatur *IPSec Policy* untuk mengenkripsi trafik yang berasal dari LAN MATARAM (192.168.1.0/24) ke LAN SUMBAWA (192.168.2.0/24) dan sebaliknya.

```
[admin@MATARAM] > ip ipsec policy add src-address=192.168.1.0/24 src-port=any dst-address=192.168.2.0/24 \
... dst-port=any sa-src-address=203.0.113.1 sa-dst-address=203.0.113.6 tunnel=yes \
... action=encrypt proposal=default
```

Penjelasan parameter:

- a) **src-address**, digunakan untuk menentukan alamat IP sumber yang harus cocok pada paket yaitu 192.168.1.0/24.
- b) **src-port**, digunakan untuk menentukan nomor *port* sumber yang harus cocok pada paket yaitu “any” yang menyatakan semua *port* sumber.
- c) **dst-address**, digunakan untuk menentukan alamat IP tujuan yang harus cocok pada paket yaitu 192.168.2.0/24.
- d) **dst-port**, digunakan untuk menentukan nomor *port* tujuan yang harus cocok pada paket yaitu “any” yang menyatakan semua *port* tujuan.
- e) **sa-src-address**, digunakan untuk menentukan alamat IP dari *Security Association (SA)* sumber yaitu 203.0.113.1 yang merupakan *local peer (router MATARAM)*.
- f) **sa-dst-address**, digunakan untuk menentukan alamat IP dari *Security Association (SA)* tujuan yaitu 203.0.113.6 yang merupakan *remote peer (router SUMBAWA)*.
- g) **tunnel**, digunakan untuk menentukan apakah menggunakan *mode tunnel* atau tidak yaitu “yes”.
- h) **action**, digunakan untuk menentukan apa yang dilakukan terhadap paket apabila cocok dengan ketentuan *policy* yaitu “encrypt”.
- i) **proposal**, digunakan untuk menentukan nama dari template proposal yang akan dikirim oleh *IKE daemon* untuk membentuk *Security Association (SA)* untuk *IPSec Policy* ini yaitu “default”.



- Memverifikasi pengaturan *IPSec Policy*.

```
[admin@MATARAM] > ip ipsec policy print
Flags: T - template, X - disabled, D - dynamic, I - inactive, * - default
0 T * group=default src-address=::/0 dst-address=::/0 protocol=all proposal=default template=yes

1      src-address=192.168.1.0/24 src-port=any dst-address=192.168.2.0/24 dst-port=any protocol=all
      action=encrypt level=require ipsec-protocols=esp tunnel=yes sa-src-address=203.0.113.1
      sa-dst-address=203.0.113.6 proposal=default priority=0
```

- Mengatur *NAT bypass rule* untuk paket dengan alamat IP sumber 192.168.1.0/24 (LAN MATARAM) dengan alamat IP tujuan 192.168.2.0/24 (LAN SUMBAWA) agar router MATARAM dapat mengenkripsi paket berdasarkan alamat sumber yang telah ditentukan pada konfigurasi *IPSec Policy* dan menempatkan *rule* ini sebelum *item number* "0" (paling atas).

```
[admin@MATARAM] > ip firewall nat add chain=srcnat action=accept place-before=0 src-address=192.168.1.0/24 \
\... dst-address=192.168.2.0/24
```

- Memverifikasi pengaturan *NAT bypass rule*.

```
[admin@MATARAM] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
0      chain=srcnat action=accept src-address=192.168.1.0/24 dst-address=192.168.2.0/24

1      chain=srcnat action=masquerade out-interface=public
```

## K. KONFIGURASI IPSEC DI ROUTER SUMBAWA

Adapun langkah-langkah konfigurasi *IPSEC VPN Tunnel* di router SUMBAWA adalah sebagai berikut:

- Melakukan pengaturan *IPSec Peer* dengan router MATARAM. *IPSec Peer* digunakan untuk membentuk koneksi antara *Internet Key Exchange (IKE) daemon* yaitu pada konfigurasi *phase 1*. Koneksi yang telah terbentuk ini akan digunakan untuk negosiasi *keys* dan algoritma untuk *Security Association (SA)*.

```
[admin@SUMBAWA] > ip ipsec peer add address=203.0.113.1 port=500 auth-method=pre-shared-key secret="12345678"
```

Penjelasan parameter:

- a) **address**, digunakan untuk menentukan alamat IP dari *remote peer* yaitu *203.0.113.1* yang merupakan alamat IP dari *router MATARAM*.
- b) **port**, digunakan untuk menentukan nomor *port* komunikasi ke *remote peer* yaitu *500*.
- c) **auth-method**, digunakan untuk menentukan metode otentikasi yaitu *pre-shared-key* yang merupakan metode otentikasi menggunakan sandi yang telah dibagi pakai antar *peer*.
- d) **secret**, digunakan untuk mengatur sandi ketika metode otentikasi yang digunakan adalah *pre-shared-key* yaitu *12345678*.

## 2. Memverifikasi pengaturan *IPSec Peer*.

```
[admin@SUMBAWA] > ip ipsec peer print
Flags: X - disabled, D - dynamic
0    address=203.0.113.1/32 local-address=:: passive=no port=500 auth-method=pre-shared-key
secret="12345678" generate-policy=no policy-template-group=default exchange-mode=main
send-initial-contact=yes nat-traversal=yes proposal-check=obey hash-algorithm=sha1
enc-algorithm=aes-128,3des dh-group=modp1024 lifetime=1d lifebytes=0 dpd-interval=2m
dpd-maximum-failures=5
```

3. Mengatur *IPSec Proposal* untuk menentukan algoritma otentikasi dan enkripsi yang digunakan oleh router. Informasi *proposal* akan dikirimkan oleh *IKE daemon* untuk membentuk *Security Association (SA)* dari *IPSec Policy* pada *phase 2*. Kedua router yaitu *MATARAM* dan *SUMBAWA* harus menggunakan algoritma yang sama. Mikrotik telah membuatkan satu *IPSec Proposal* dengan nama "**default**" yang menggunakan algoritma otentikasi "**sha1**" dan algoritma enkripsi "**aes-256-cbc,aes-192-cbc,aes-128-cbc**" dimana masing-masing ditunjukkan pada parameter *auth-algorithms* dan *enc-algorithms*.

```
[admin@SUMBAWA] > ip ipsec proposal print
Flags: X - disabled, * - default
0 * name="default" auth-algorithms=sha1 enc-algorithms=aes-256-cbc,aes-192-cbc,aes-128-cbc lifetime=30m
pfs-group=modp1024
```

Studi kasus konfigurasi *Site-to-Site IPsec VPN Tunnel* ini menggunakan proposal “default”.

4. Mengatur *IPsec Policy* untuk mengenkripsi trafik yang berasal dari LAN SUMBAWA (192.168.2.0/24) ke LAN MATARAM (192.168.1.0/24) dan sebaliknya.

```
[admin@SUMBAWA] > ip ipsec policy add src-address=192.168.2.0/24 src-port=any dst-address=192.168.1.0/24 \
... dst-port=any sa-src-address=203.0.113.6 sa-dst-address=203.0.113.1 tunnel=yes \
... action=encrypt proposal=default
```

Penjelasan parameter:

- a) **src-address**, digunakan untuk menentukan alamat IP sumber yang harus cocok pada paket yaitu 192.168.1.0/24.
- b) **src-port**, digunakan untuk menentukan nomor *port* sumber yang harus cocok pada paket yaitu “any” yang menyatakan semua *port* sumber.
- c) **dst-address**, digunakan untuk menentukan alamat IP tujuan yang harus cocok pada paket yaitu 192.168.2.0/24.
- d) **dst-port**, digunakan untuk menentukan nomor *port* tujuan yang harus cocok pada paket yaitu “any” yang menyatakan semua *port* tujuan.
- e) **sa-src-address**, digunakan untuk menentukan alamat IP dari *Security Association (SA)* sumber yaitu 203.0.113.1 yang merupakan *local peer (router MATARAM)*.
- f) **sa-dst-address**, digunakan untuk menentukan alamat IP dari *Security Association (SA)* tujuan yaitu 203.0.113.6 yang merupakan *remote peer (router SUMBAWA)*.
- g) **tunnel**, digunakan untuk menentukan apakah menggunakan *mode tunnel* atau tidak yaitu “yes”.

- h) **action**, digunakan untuk menentukan apa yang dilakukan terhadap paket apabila cocok dengan ketentuan *policy* yaitu "encrypt".
- i) **proposal**, digunakan untuk menentukan nama dari template proposal yang akan dikirim oleh *IKE daemon* untuk membentuk *Security Association (SA)* untuk *IPSec Policy* ini yaitu "default".

5. Memverifikasi pengaturan *IPSec Policy*.

```
[admin@SUMBAWA] > ip ipsec policy print
Flags: T - template, X - disabled, D - dynamic, I - inactive, * - default
0 T * group=default src-address=::/0 dst-address=::/0 protocol=all proposal=default template=yes

1   src-address=192.168.2.0/24 src-port=any dst-address=192.168.1.0/24 dst-port=any protocol=all
    action=encrypt level=require ipsec-protocols=esp tunnel=yes sa-src-address=203.0.113.6
    sa-dst-address=203.0.113.1 proposal=default priority=0
```

6. Mengatur *NAT bypass rule* untuk paket dengan alamat IP sumber 192.168.2.0/24 (LAN SUMBAWA) dengan alamat IP tujuan 192.168.1.0/24 (LAN MATARAM) agar router SUMBAWA dapat mengenkripsi paket berdasarkan alamat sumber yang telah ditentukan pada konfigurasi *IPSec Policy* dan menempatkan *rule* ini sebelum *item number* "0" (paling atas).

```
[admin@SUMBAWA] > ip firewall nat add chain=srcnat action=accept place-before=0 src-address=192.168.2.0/24 \
\... dst-address=192.168.1.0/24
```

7. Memverifikasi pengaturan *NAT bypass rule*.

```
[admin@SUMBAWA] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
0   chain=srcnat action=accept src-address=192.168.2.0/24 dst-address=192.168.1.0/24

1   chain=srcnat action=masquerade out-interface=public
```

## L. VERIFIKASI KONEKSI ANTAR PC DI LAN MATARAM DENGAN PC DI LAN SURABAYA

Adapun langkah-langkah verifikasi koneksi antar PC di LAN MATARAM dengan PC di LAN SUMBAWA adalah sebagai berikut:

1. Memverifikasi koneksi dari *VPCS PC1* yang terdapat di LAN MATARAM ke *VPCS PC3* yang terdapat di LAN SUMBAWA menggunakan perintah *ping*.

```
PC1> ping 192.168.2.253
84 bytes from 192.168.2.253 icmp_seq=1 ttl=62 time=130.083 ms
84 bytes from 192.168.2.253 icmp_seq=2 ttl=62 time=95.063 ms
84 bytes from 192.168.2.253 icmp_seq=3 ttl=62 time=133.084 ms
84 bytes from 192.168.2.253 icmp_seq=4 ttl=62 time=86.053 ms
84 bytes from 192.168.2.253 icmp_seq=5 ttl=62 time=131.085 ms
```

Koneksi telah berhasil dilakukan.

2. Memverifikasi koneksi dari *VPCS PC1* yang terdapat di LAN MATARAM ke *VPCS PC4* yang terdapat di LAN SUMBAWA menggunakan perintah *ping*.

```
PC1> ping 192.168.2.254
84 bytes from 192.168.2.254 icmp_seq=1 ttl=62 time=73.049 ms
84 bytes from 192.168.2.254 icmp_seq=2 ttl=62 time=140.095 ms
84 bytes from 192.168.2.254 icmp_seq=3 ttl=62 time=116.078 ms
84 bytes from 192.168.2.254 icmp_seq=4 ttl=62 time=129.082 ms
84 bytes from 192.168.2.254 icmp_seq=5 ttl=62 time=80.048 ms
```

Koneksi telah berhasil dilakukan.

3. Memverifikasi koneksi dari *VPCS PC2* yang terdapat di LAN MATARAM ke *VPCS PC3* yang terdapat di LAN SUMBAWA menggunakan perintah *ping*.

```
PC2> ping 192.168.2.253
84 bytes from 192.168.2.253 icmp_seq=1 ttl=62 time=110.055 ms
84 bytes from 192.168.2.253 icmp_seq=2 ttl=62 time=155.100 ms
84 bytes from 192.168.2.253 icmp_seq=3 ttl=62 time=123.082 ms
84 bytes from 192.168.2.253 icmp_seq=4 ttl=62 time=95.065 ms
84 bytes from 192.168.2.253 icmp_seq=5 ttl=62 time=96.059 ms
```

Koneksi telah berhasil dilakukan.

4. Memverifikasi koneksi dari *VPCS PC2* yang terdapat di LAN MATARAM ke *VPCS PC4* yang terdapat di LAN SUMBAWA menggunakan perintah *ping*.

```
PC2> ping 192.168.2.254
84 bytes from 192.168.2.254 icmp_seq=1 ttl=62 time=121.081 ms
84 bytes from 192.168.2.254 icmp_seq=2 ttl=62 time=110.069 ms
84 bytes from 192.168.2.254 icmp_seq=3 ttl=62 time=137.089 ms
84 bytes from 192.168.2.254 icmp_seq=4 ttl=62 time=136.089 ms
84 bytes from 192.168.2.254 icmp_seq=5 ttl=62 time=112.074 ms
```

Koneksi telah berhasil dilakukan.

Selamat Anda telah berhasil mengkonfigurasi *Site-to-Site IPSec VPN Tunnel* di Mikrotik ☺. Apabila terdapat pertanyaan, jangan segan untuk bertanya melalui email pada alamat [admin@iputuhariyadi.net](mailto:admin@iputuhariyadi.net). Semoga bermanfaat. Terimakasih.

Sumber Referensi: Wiki Mikrotik, <http://wiki.mikrotik.com>