JUNIPER

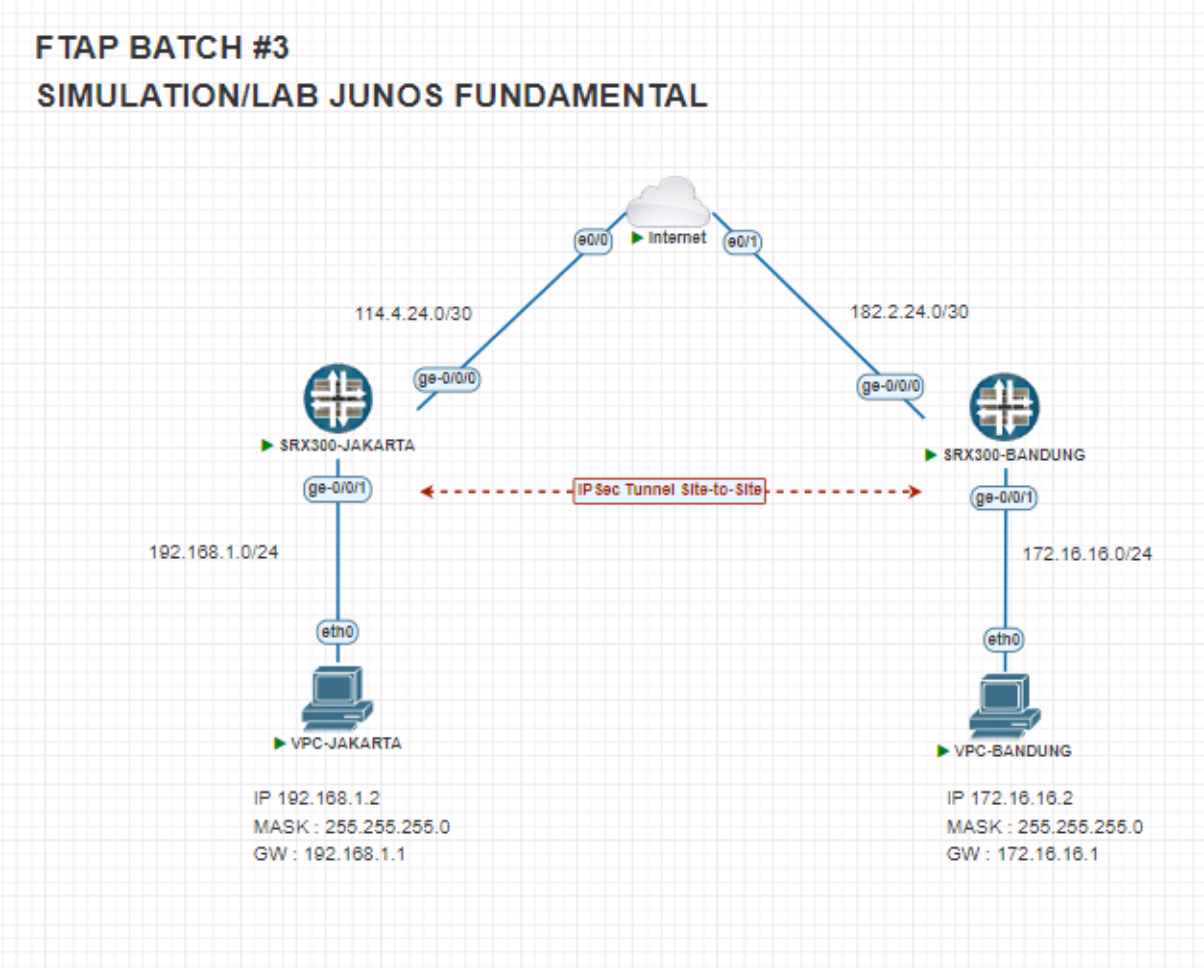
05 – SIMULATION/LAB JUNOS FUNDAMENTAL

- ✓ Konfigrasi (IPSec Tunnel Site-to-Site).
- ✓ Pengujian dan Verifikasi.

Annisa Hadita

Mentor: Dito Prasetya

1. **Topology**



2. **Task**

Task ini melakukan IPSec Site-to-Site dengan membuat jalur aman (tunnel) melalui internet publik untuk mengamankan komunikasi antara dua jaringan yang berbeda. Dengan menggunakan IPsec VPN, data yang dikirimkan antara dua jaringan akan dienkripsi sehingga dapat memastikan keamanan data.

#Configuration IP Address SRX300

Perintah ge-0/0/0 digunakan untuk menghubungkan router ke jaringan internet dengan menggunakan alamat IP publik. Interface ini digunakan untuk koneksi ke ISP (internet).

Perintah ge-0/0/1 digunakan untuk menghubungkan router ke jaringan LAN dengan menggunakan alamat IP private.

SRX300-JAKARTA

```
set interfaces ge-0/0/0 unit 0 family inet address 114.4.24.2/30
```

set interfaces ge-0/0/1 unit 0 family inet address 192.168.1.1/24

```
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 114.4.24.2/30;
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family inet {
                address 192.168.1.1/24;
            }
        }
    }
```

SRX300-BANDUNG

set interfaces ge-0/0/0 unit 0 family inet address 182.2.24.2/30

set interfaces ge-0/0/1 unit 0 family inet address 172.16.16.1/24

```
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 182.2.24.2/30;
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family inet {
                address 172.16.16.1/24;
            }
        }
    }
```

#Configuration Default Route

Perintah ini digunakan untuk memastikan bahwa koneksi antara Jakarta dan Bandung melalui IP Public dan dapat saling terhubung untuk koneksi IPSec Tunnel, sehingga dapat berkomunikasi melalui jalur public atau internet.

SRX300-JAKARTA

```
set routing-options static route 0.0.0.0/0 next-hop 114.4.24.1
```

```
routing-options {
    static {
        route 0.0.0.0/0 next-hop 114.4.24.1;
```

SRX300-BANDUNG

```
set routing-options static route 0.0.0.0/0 next-hop 182.2.24.1
```

```
routing-options {
    static {
        route 0.0.0.0/0 next-hop 182.2.24.1;
```

#Configure IPSec Tunnel Site-to-Site

- **Interfaces Tunnel (St.0) SRX300-JAKARTA & SRX300-BANDUNG**

```
set interfaces st0 unit 0 family inet
set interfaces st0.0 family inet address 10.1.1.1/30 (SRX300-Jakarta)
set interfaces st0.0 family inet address 10.1.1.2/30 (SRX300-Bandung)
```

Perintah in digunakan untuk mengkonfigurasi interface (st0) yang berfungsi sebagai tunnel IPsec Site-to-Site VPN untuk membuat jalur aman antara dua jaringan yang berbeda melalui internet publik.

SRX300-JAKARTA

```
    st0 {
        unit 0 {
            family inet {
                address 10.1.1.1/30;
            }
        }
    }
```

SRX300-BANDUNG

```
    st0 {
        unit 0 {
            family inet {
                address 10.1.1.2/30;
            }
        }
    }
```

- **Phase1**

SRX300-JAKARTA

```
set security ike proposal IKE-PROPOSAL authentication-method pre-shared-keys
set security ike proposal IKE-PROPOSAL dh-group group5
set security ike proposal IKE-PROPOSAL authentication-algorithm sha-256
set security ike proposal IKE-PROPOSAL encryption-algorithm 3des-cbc
set security ike proposal IKE-PROPOSAL lifetime-seconds 86400
```

Perintah ini digunakan untuk mengatur proposal IKE (Internet Key Exchange) membuat IPsec Site-to-Site VPN dan memastikan bahwa terowongan VPN memiliki tingkat keamanan yang tinggi melalui autentikasi dan enkripsi.

```
security {
    ike {
        proposal IKE-PROPOSAL {
            authentication-method pre-shared-keys;
            dh-group group5;
            authentication-algorithm sha-256;
            encryption-algorithm 3des-cbc;
            lifetime-seconds 86400;
        }
```

```
set security ike policy IKE-POLICY mode main
set security ike policy IKE-POLICY proposals IKE-PROPOSAL
set security ike policy IKE-POLICY pre-shared-key ascii-text ftap3
```

Perintah ini digunakan untuk memastikan bahwa kebijakan IKE memiliki pengaturan keamanan yang telah dibuat sehingga Jakarta dan Bandung dapat berkomunikasi melalui terowongan VPN yang terenkripsi.

```
policy IKE-POLICY {
    mode main;
    proposals IKE-PROPOSAL;
    pre-shared-key ascii-text "$9$v4d8X-s2aZGiVwP5"; ## SECRET-DATA
}
```

```
set security ike gateway IKE-GATEWAY ike-policy IKE-POLICY
set security ike gateway IKE-GATEWAY address 182.2.24.2
set security ike gateway IKE-GATEWAY external-interface ge-0/0/0
set security ike gateway IKE-GATEWAY version v2-only
```

Perintah ini digunakan untuk menjalankan IPsec Site-to-Site VPN dengan aman yang menghubungkan kebijakan IKE, menentukan alamat IP address untuk membentuk terowongan VPN yang terenkripsi dengan keamanan tinggi antara dua lokasi yang berbeda.

```
gateway IKE-GATEWAY {
    ike-policy IKE-POLICY;
    address 182.2.24.2;
    external-interface ge-0/0/0;
    version v2-only;
}
```

SRX300-BANDUNG

```
set security ike proposal IKE-PROPOSAL authentication-method pre-shared-keys
set security ike proposal IKE-PROPOSAL dh-group group5
set security ike proposal IKE-PROPOSAL authentication-algorithm sha-256
set security ike proposal IKE-PROPOSAL encryption-algorithm 3des-cbc
set security ike proposal IKE-PROPOSAL lifetime-seconds 86400
```

Perintah ini digunakan untuk mengatur proposal IKE (Internet Key Exchange) membuat IPsec Site-to-Site VPN dan memastikan bahwa terowongan VPN memiliki tingkat keamanan yang tinggi melalui autentikasi dan enkripsi.

```
security {
    ike {
        proposal IKE-PROPOSAL {
            authentication-method pre-shared-keys;
            dh-group group5;
            authentication-algorithm sha-256;
            encryption-algorithm 3des-cbc;
            lifetime-seconds 86400;
        }
```

```
set security ike policy IKE-POLICY mode main
set security ike policy IKE-POLICY proposals IKE-PROPOSAL
set security ike policy IKE-POLICY pre-shared-key ascii-text ftap3
```

Perintah ini digunakan untuk memastikan bahwa kebijakan IKE memiliki pengaturan keamanan yang telah dibuat sehingga Jakarta dan Bandung dapat berkomunikasi melalui terowongan VPN yang terenkripsi.

```
policy IKE-POLICY {
    mode main;
    proposals IKE-PROPOSAL;
    pre-shared-key ascii-text "$9$paN2OlhlK8XxdSr24"; ## SECRET-DATA
}
```

```
set security ike gateway IKE-GATEWAY ike-policy IKE-POLICY
set security ike gateway IKE-GATEWAY address 114.4.24.2
set security ike gateway IKE-GATEWAY external-interface ge-0/0/0
set security ike gateway IKE-GATEWAY version v2-only
```

Perintah ini digunakan untuk menjalankan IPsec Site-to-Site VPN dengan aman yang menghubungkan kebijakan IKE, menentukan alamat IP address untuk membentuk terowongan VPN yang terenkripsi dengan keamanan tinggi antara dua lokasi yang berbeda.

```
gateway IKE-GATEWAY {
    ike-policy IKE-POLICY;
    address 114.4.24.2;
    external-interface ge-0/0/0;
    version v2-only;
}
```

- **Phase2**

  SRX300-JAKARTA

```
set security ipsec proposal IPSEC-PROPOSAL protocol esp
set security ipsec proposal IPSEC-PROPOSAL authentication-algorithm hmac-sha1-96
set security ipsec proposal IPSEC-PROPOSAL encryption-algorithm 3des-cbc
```

```
set security ipsec proposal IPSEC-PROPOSAL lifetime-seconds 28800
```

Perintah ini digunakan untuk menetapkan proposal IPsec dengan pengaturan yang sesuai untuk memastikan keamanan data.

```
ipsec {
    proposal IPSEC-PROPOSAL {
        protocol esp;
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm 3des-cbc;
        lifetime-seconds 28800;
    }
```

```
set security ipsec vpn IPSEC-VPN-BANDUNG bind-interface st0.0
set security ipsec vpn IPSEC-VPN-BANDUNG ike gateway IKE-GATEWAY
set security ipsec vpn IPSEC-VPN-BANDUNG ike ipsec-policy IPSEC-POLICY
set security ipsec vpn IPSEC-VPN-BANDUNG establish-tunnels immediately
```

Konfigurasi ini digunakan untuk membuat semacam jaringan pribadi virtual (VPN) yang aman antara dua lokasi yang berbeda sehingga dapat memastikan bahwa komunikasi antara Jakarta dan Bandung melalui internet aman.

```
vpn IPSEC-VPN-JAKARTA {
    bind-interface st0.0;
    ike {
        gateway IKE-GATEWAY;
        ipsec-policy IPSEC-POLICY;
    }
    establish-tunnels immediately;
}
```

SRX300-BANDUNG

```
set security ipsec proposal IPSEC-PROPOSAL protocol esp
set security ipsec proposal IPSEC-PROPOSAL authentication-algorithm hmac-sha1-96
set security ipsec proposal IPSEC-PROPOSAL encryption-algorithm 3des-cbc
set security ipsec proposal IPSEC-PROPOSAL lifetime-seconds 28800
```

Perintah ini digunakan untuk menetapkan proposal IPsec dengan pengaturan yang sesuai untuk memastikan keamanan data.

```
ipsec {
    proposal IPSEC-PROPOSAL {
        protocol esp;
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm 3des-cbc;
        lifetime-seconds 28800;
    }
```

```
set security ipsec vpn IPSEC-VPN-JAKARTA bind-interface st0.0
set security ipsec vpn IPSEC-VPN-JAKARTA ike gateway IKE-GATEWAY
set security ipsec vpn IPSEC-VPN-JAKARTA ike ipsec-policy IPSEC-POLICY
set security ipsec vpn IPSEC-VPN-JAKARTA establish-tunnels immediately
```

Konfigurasi ini digunakan untuk membuat semacam jaringan pribadi virtual (VPN) yang aman antara dua lokasi yang berbeda sehingga dapat memastikan bahwa komunikasi antara Jakarta dan Bandung melalui internet aman.

```
vpn IPSEC-VPN-JAKARTA {
    bind-interface st0.0;
    ike {
        gateway IKE-GATEWAY;
        ipsec-policy IPSEC-POLICY;
    }
    establish-tunnels immediately;
}
```

- **Zone Trust (Interface ke LAN) SRX300-JAKARTA & SRX300-BANDUNG**

```
set security zones security-zone TRUST host-inbound-traffic system-services all
set security zones security-zone TRUST host-inbound-traffic protocols all
set security zones security-zone TRUST interfaces ge-0/0/1.0
```

Konfigurasi ini digunakan untuk menetapkan aturan keamanan pada zona keamanan "TRUST" (wilayah di dalam perangkat yang memiliki kebijakan keamanan). Perangkat yang terhubung ke interface ge-0/0/1.0 memiliki akses ke layanan sistem dan protokol yang diizinkan.

```
zones {
    security-zone TRUST {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-0/0/1.0;
        }
    }
```

- **Zone Untrust (Interface ke Internet) SRX300-JAKARTA & SRX300-BANDUNG**

```
set security zones security-zone UNTRUST host-inbound-traffic system-services all
set security zones security-zone UNTRUST host-inbound-traffic protocols all
set security zones security-zone UNTRUST interfaces ge-0/0/0.0
```

Konfigurasi ini digunakan untuk menetapkan aturan keamanan pada zona keamanan " UNTRUST" (wilayah di dalam perangkat yang memiliki kebijakan keamanan). Perangkat yang terhubung ke interface ge-0/0/0.0 memiliki akses ke layanan sistem dan protokol yang diizinkan.

```
  security-zone UNTRUST {
      host-inbound-traffic {
          system-services {
              all;
          }
          protocols {
              all;
          }
      }
      interfaces {
          ge-0/0/0.0;
      }
  }
```

- **Zone VPN (Interface Tunnel) SRX300-JAKARTA & SRX300-BANDUNG**

```
set security zones security-zone VPN host-inbound-traffic system-services all
set security zones security-zone VPN host-inbound-traffic protocols all
set security zones security-zone VPN interfaces st0.0
```

Konfigurasi ini digunakan untuk menetapkan aturan keamanan pada zona keamanan " VPN" yang digunakan untuk memfasilitasi koneksi melalui jalur terowongan (tunnel) VPN antara kedua perangkat.

```
    security-zone VPN {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            st0.0;
        }
    }
```

- **Policy dari Zone Untrust to Untrust SRX300-JAKARTA & SRX300-BANDUNG**

```
set security policies from-zone UNTRUST to-zone UNTRUST policy default-deny match source-address any
set security policies from-zone UNTRUST to-zone UNTRUST policy default-deny match destination-address any
set security policies from-zone UNTRUST to-zone UNTRUST policy default-deny match application any
set security policies from-zone UNTRUST to-zone UNTRUST policy default-deny then permit
```

Konfigurasi ini digunakan untuk menetapkan kebijakan keamanan dari zona keamanan "UNTRUST" ke zona keamanan "UNTRUST" pada perangkat dan memastikan bahwa hanya traffic yang diizinkan secara khusus yang dapat berkomunikasi melalui zona ini, sementara yang lainnya akan ditolak.

```
policies {
    from-zone UNTRUST to-zone UNTRUST {
        policy default-deny {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
```

- **Policy dari Zone VPN to Trust SRX300-JAKARTA & SRX300-BANDUNG**

```
set security policies from-zone VPN to-zone TRUST policy default-deny match source-address any
set security policies from-zone VPN to-zone TRUST policy default-deny match destination-address any
set security policies from-zone VPN to-zone TRUST policy default-deny match application any
set security policies from-zone VPN to-zone TRUST policy default-deny then permit
```

Konfigurasi ini digunakan untuk menetapkan kebijakan keamanan default dari zona "VPN" ke zona "TRUST" pada perangkat. Zona keamanan VPN diatur untuk memiliki aturan keamanan yang ketat dan memastikan bahwa hanya lalu lintas yang diizinkan secara khusus yang dapat berkomunikasi dengan zona TRUST.

```
from-zone VPN to-zone TRUST {
    policy default-deny {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
```

- **Policy dari Zone Trust to VPN SRX300-JAKARTA & SRX300-BANDUNG**

```
set security policies from-zone TRUST to-zone VPN policy default-deny match source-address any
set security policies from-zone TRUST to-zone VPN policy default-deny match destination-address any
set security policies from-zone TRUST to-zone VPN policy default-deny match application any
set security policies from-zone TRUST to-zone VPN policy default-deny then permit
```

Konfigurasi ini digunakan untuk menetapkan kebijakan keamanan default dari zona "TRUST" ke zona "VPN" pada perangkat dan memastikan bahwa hanya trrafic yang diizinkan yang dapat berkomunikasi dengan zona VPN, sementara yang lainnya akan ditolak.

```
from-zone TRUST to-zone VPN {
    policy default-deny {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
```

- **Static Routing**

  Konfigurasi ini digunakan untuk memastikan bahwa traffic yang ditujukan ke subnet 172.16.16.0/24 atau 192.168.1.0/24 diteruskan melalui jalur yang telah ditentukan melalui terowongan (tunnel) st0.0. Terowongan (tunnel) st0.0 digunakan untuk mengarahkan traffic melalui jalur VPN (Virtual Private Network), yang memungkinkan komunikasi aman antara lokasi jaringan yang berbeda melalui internet publik.

  SRX300-JAKARTA

```
set routing-options static route 172.16.16.0/24 next-hop st0.0
```

```
    route 172.16.16.0/24 next-hop st0.0;
}
```

  SRX300-BANDUNG

```
set routing-options static route 192.168.1.0/24 next-hop st0.0
```

```
    route 192.168.1.0/24 next-hop st0.0;
}
```

#Configure IP VPC

SRX300-JAKARTA

```
ip 192.168.1.2/24 192.168.1.1
```

```
NAME    IP/MASK              GATEWAY                          GATEWAY
VPCS1   192.168.1.2/24       192.168.1.1
        fe80::250:79ff:fe66:6812/64
```

SRX300-BANDUNG

```
ip 192.168.1.2/24 192.168.1.1
```

```
NAME    IP/MASK              GATEWAY                          GATEWAY
VPCS1   192.168.1.2/24       192.168.1.1
        fe80::250:79ff:fe66:6812/64
```

3. Verifikasi

- **Phase 1 SRX300-JAKARTA & SRX300-BANDUNG**

show security ike security-associations

```
root@SRX300-JAKARTA> show security ike security-associations
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address
4231800 UP     dea5a2877b112040  ffa57631d275e1f2  IKEv2          182.2.24.2
```

show security ike security-associations detail

```
root@SRX300-JAKARTA> show security ike security-associations detail
IKE peer 182.2.24.2, Index 4231800, Gateway Name: IKE-GATEWAY
  Role: Responder, State: UP
  Initiator cookie: dea5a2877b112040, Responder cookie: ffa57631d275e1f2
  Exchange type: IKEv2, Authentication method: Pre-shared-keys
  Local: 114.4.24.2:500, Remote: 182.2.24.2:500
  Lifetime: Expires in 21375 seconds
  Peer ike-id: 182.2.24.2
  Xauth assigned IP: 0.0.0.0
  Algorithms:
   Authentication        : hmac-sha256-128
   Encryption            : 3des-cbc
   Pseudo random function: hmac-sha256
   Diffie-Hellman group  : DH-group-5
  Traffic statistics:
   Input  bytes  :                 1238
   Output bytes  :                 1198
   Input  packets:                    6
   Output packets:                    6
  Flags: IKE SA is created
  IPSec security associations: 6 created, 0 deleted
  Phase 2 negotiations in progress: 0

    Negotiation type: Quick mode, Role: Responder, Message ID: 0
    Local: 114.4.24.2:500, Remote: 182.2.24.2:500
    Local identity: 114.4.24.2
    Remote identity: 182.2.24.2
    Flags: IKE SA is created
```

show security ike security-associations

```
root@SRX300-BANDUNG> show security ike security-associations
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address
6092677 UP     dea5a2877b112040  ffa57631d275e1f2  IKEv2          114.4.24.2
```

show security ipsec security-associations detail

```
root@SRX300-BANDUNG> show security ike security-associations detail
IKE peer 114.4.24.2, Index 6092677, Gateway Name: IKE-GATEWAY
  Role: Initiator, State: UP
  Initiator cookie: dea5a2877b112040, Responder cookie: ffa57631d275e1f2
  Exchange type: IKEv2, Authentication method: Pre-shared-keys
  Local: 182.2.24.2:500, Remote: 114.4.24.2:500
  Lifetime: Expires in 21335 seconds
  Peer ike-id: 114.4.24.2
  Xauth assigned IP: 0.0.0.0
  Algorithms:
   Authentication        : hmac-sha256-128
   Encryption            : 3des-cbc
   Pseudo random function: hmac-sha256
   Diffie-Hellman group  : DH-group-5
  Traffic statistics:
   Input  bytes  :                 1198
   Output bytes  :                 1238
   Input  packets:                    6
   Output packets:                    6
  Flags: IKE SA is created
  IPSec security associations: 6 created, 2 deleted
  Phase 2 negotiations in progress: 0

    Negotiation type: Quick mode, Role: Initiator, Message ID: 0
    Local: 182.2.24.2:500, Remote: 114.4.24.2:500
    Local identity: 182.2.24.2
    Remote identity: 114.4.24.2
    Flags: IKE SA is created
```

4. **Pengujian**

- **VPC-JAKARTA to VPC-BANDUNG**

```
VPCS> ping 172.16.16.2

84 bytes from 172.16.16.2 icmp_seq=1 ttl=62 time=51.440 ms
84 bytes from 172.16.16.2 icmp_seq=2 ttl=62 time=12.364 ms
84 bytes from 172.16.16.2 icmp_seq=3 ttl=62 time=13.688 ms
84 bytes from 172.16.16.2 icmp_seq=4 ttl=62 time=14.322 ms
84 bytes from 172.16.16.2 icmp_seq=5 ttl=62 time=12.757 ms
```

- **Verifikasi Site SRX300-BANDUNG**

  show security flow session source-prefix 192.168.1.2 destination-prefix 172.16.16.2

```
root@SRX300-BANDUNG> ...refix 192.168.1.2 destination-prefix 172.16.16.2
Session ID: 34, Policy name: default-deny/5, Timeout: 2, Valid
  In: 192.168.1.2/1 --> 172.16.16.2/26452;icmp, If: st0.0, Pkts: 1, Bytes: 84
  Out: 172.16.16.2/26452 --> 192.168.1.2/1;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes: 84

Session ID: 35, Policy name: default-deny/5, Timeout: 4, Valid
  In: 192.168.1.2/2 --> 172.16.16.2/26708;icmp, If: st0.0, Pkts: 1, Bytes: 84
  Out: 172.16.16.2/26708 --> 192.168.1.2/2;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes: 84
Total sessions: 2
```

- **VPC-BANDUNG to VPC-JAKARTA**

```
VPCS> ping 192.168.1.2

84 bytes from 192.168.1.2 icmp_seq=1 ttl=62 time=19.807 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=62 time=12.795 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=62 time=16.069 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=62 time=13.198 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=62 time=7.499 ms
```

- **Verifikasi Site SRX300-JAKARTA**

  show security flow session source-prefix 192.168.1.2 destination-prefix 172.16.16.2

```
root@SRX300-JAKARTA> ...refix 172.16.16.2 destination-prefix 192.168.1.2
Session ID: 19, Policy name: default-deny/5, Timeout: 2, Valid
  In: 172.16.16.2/1 --> 192.168.1.2/8020;icmp, If: st0.0, Pkts: 1, Bytes: 84
  Out: 192.168.1.2/8020 --> 172.16.16.2/1;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes: 84

Session ID: 20, Policy name: default-deny/5, Timeout: 2, Valid
  In: 172.16.16.2/2 --> 192.168.1.2/8276;icmp, If: st0.0, Pkts: 1, Bytes: 84
  Out: 192.168.1.2/8276 --> 172.16.16.2/2;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes: 84
Total sessions: 2
```