JUNIPER

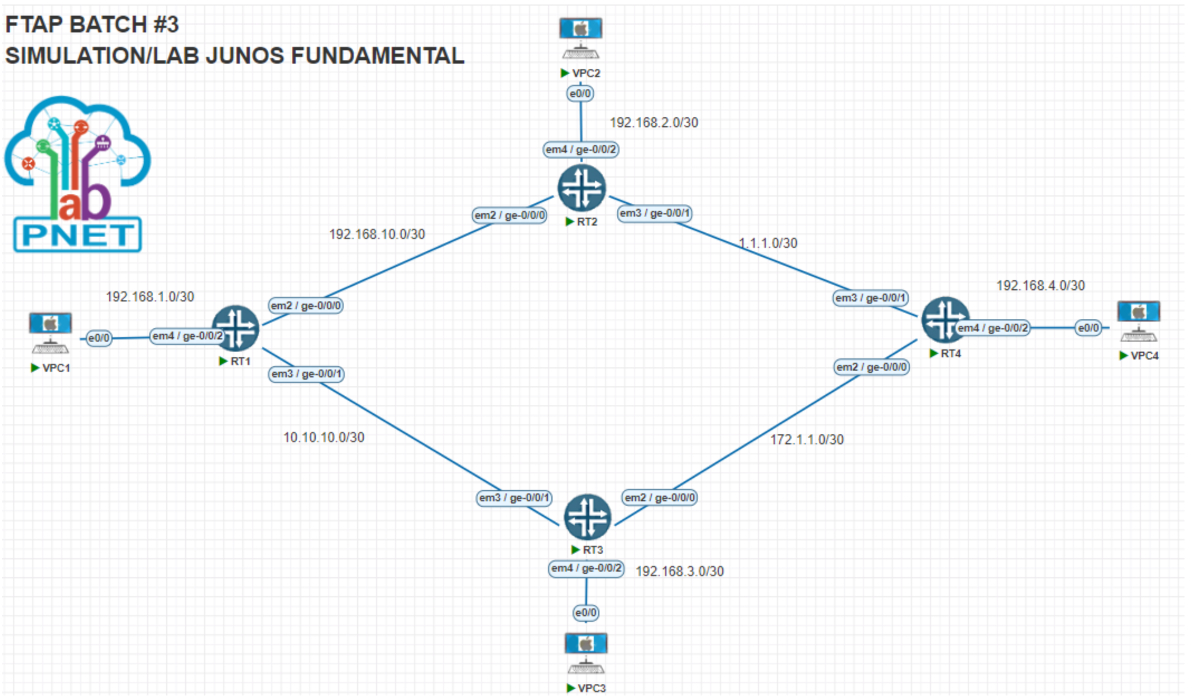
04 – SIMULATION/LAB JUNOS FUNDAMENTAL

- ✓ Konfigrasi Firewall Filter (Blocking ICMP & SSH).
- ✓ Pengujian.

Annisa Hadita

Mentor: Dito Prasetya

1. Topology



2. Task

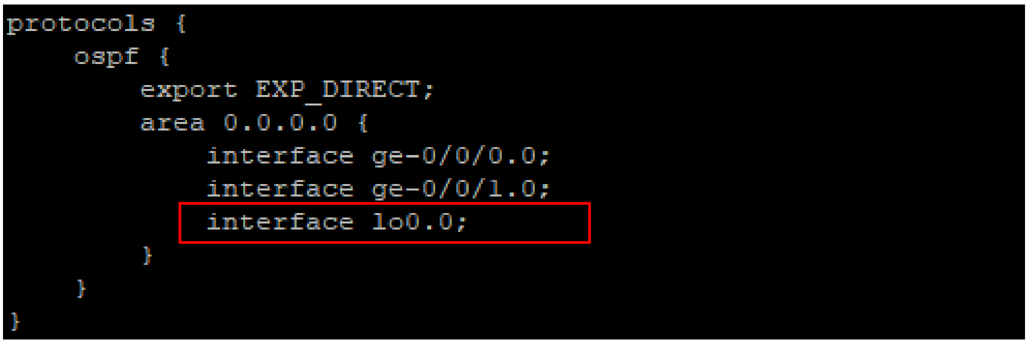
- Konfigurasi Firewall Filtering Traffic & Remote SSH.

  Task ini termasuk dalam kategori Firewall Filtering yang bertujuan untuk mengatur atau mencegah traffic masuk dan keluar yang tidak diinginkan. Misalnya, untuk melakukan keamanan akses Remote SSH. Dalam percobaan ini, akan menolak traffic yang berasal dari VPC4 yang mencoba berkomunikasi dengan R1 dan mengakses remote SSH pada R1. Konfigurasi ini akan dilakukan pada R1 dengan menggunakan alamat IP LAN.

  #Configuration Interface Loopback OSPF

  ```
  set protocols ospf area 0.0.0.0 interface lo0.0
  ```

  Perintah ini digunakan untuk menambahkan interface loopback ke dalam area OSPF dengan ID area 0.0.0.0.



```
protocols {
    ospf {
        export EXP_DIRECT;
        area 0.0.0.0 {
            interface ge-0/0/0.0;
            interface ge-0/0/1.0;
            interface lo0.0;
        }
    }
}
```

#Configuration Interface Loopback

```
set interfaces lo0 unit 0 family inet address 100.100.100.100/32
```

Perintah ini digunakan untuk menambahkan alamat IP 100.100.100.100/32 ke interface loopback pada router.

```
set interfaces lo0 unit 0 family inet address 100.100.100.100/32
```

```
set interfaces lo0 unit 0 family inet filter input block-ping
```

Perintah ini digunakan untuk memblokir permintaan ping.

```
set interfaces lo0 unit 0 family inet filter input block-ping
```

```
set interfaces lo0 unit 0 family inet filter input block-ssh
```

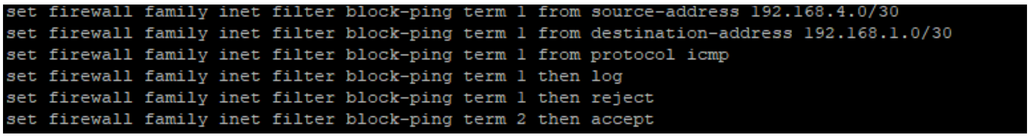
Perintah ini digunakan untuk memblokir permintaan SSH.

```
set interfaces lo0 unit 0 family inet filter input block-ssh
```

#Configure Firewall Filters Blok-Ping

```
set firewall family inet filter block-ping term 1 from source-address 192.168.4.0/30
set firewall family inet filter block-ping term 1 from destination-address 192.168.1.0/30
set firewall family inet filter block-ping term 1 from protocol icmp
set firewall family inet filter block-ping term 1 then log
set firewall family inet filter block-ping term 1 then reject
set firewall family inet filter block-ping term 2 then accept
```

Perintah ini digunakan untuk membuat sebuah firewall filter yang disebut "block-ping". Paket ICMP (yang biasanya digunakan untuk melakukan ping) akan ditolak jika berasal dari jaringan 192.168.4.0/30 (IP LAN R4 ke VPC4) dan ditujukan ke jaringan 192.168.1.0/30 (IP LAN R1 ke VPC1).

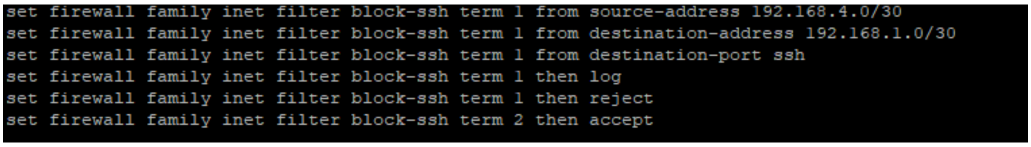


```
set firewall family inet filter block-ping term 1 from source-address 192.168.4.0/30
set firewall family inet filter block-ping term 1 from destination-address 192.168.1.0/30
set firewall family inet filter block-ping term 1 from protocol icmp
set firewall family inet filter block-ping term 1 then log
set firewall family inet filter block-ping term 1 then reject
set firewall family inet filter block-ping term 2 then accept
```

#Configure Firewall Filters Blok-SSH

```
set firewall family inet filter block-ssh term 1 from source-address 192.168.4.0/30
set firewall family inet filter block-ssh term 1 from destination-address 192.168.1.0/30
set firewall family inet filter block-ssh term 1 from protocol tcp
set firewall family inet filter block-ssh term1 from destination-port ssh
set firewall family inet filter block-ssh term 1 then log
set firewall family inet filter block-ssh term 1 then reject
set firewall family inet filter block-ssh term 2 then accept
```

Perintah ini digunakan untuk membuat sebuah firewall filter yang disebut "block-ssh". Paket TCP yang menuju port SSH akan ditolak jika berasal dari jaringan 192.168.4.0/30 (IP LAN R4 ke VPC4) dan ditujukan ke jaringan 192.168.1.0/30 (IP LAN R1 ke VPC1).



```
set firewall family inet filter block-ssh term 1 from source-address 192.168.4.0/30
set firewall family inet filter block-ssh term 1 from destination-address 192.168.1.0/30
set firewall family inet filter block-ssh term 1 from destination-port ssh
set firewall family inet filter block-ssh term 1 then log
set firewall family inet filter block-ssh term 1 then reject
set firewall family inet filter block-ssh term 2 then accept
```

#Configure Firewall Filters Blok-SSH

```
set policy-options prefix-list block-ssh-telnet 192.168.4.0/30
```

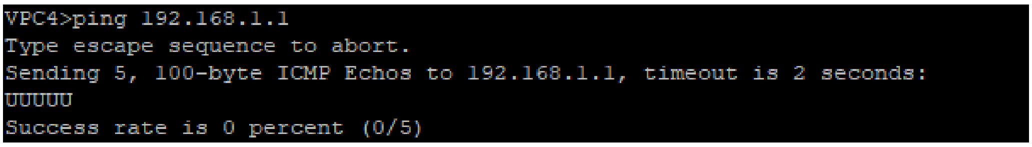
Perintah ini digunakan untuk membuat daftar prefix agar dapat memblokir atau membatasi akses SSH dan Telnet dari IP Address yang tercantum.

```
set policy-options prefix-list block-ssh-telnet 192.168.4.0/30
```

3. Pengujian Konektivitas

Pengujian ini dilakukan untuk memastikan bahwa konfigurasi firewall filter yang disebut "block-ping" berfungsi dengan baik dalam memblokir atau menolak traffic yang berasal dari IP 192.168.4.0 (IP LAN R4 ke VPC4) dan menuju ke alamat jaringan 192.168.1.0 (IP LAN R1 ke VPC1).

- **VPC4 to R1**

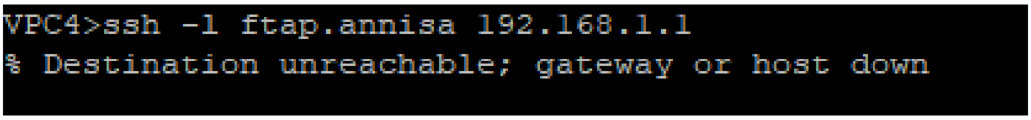


```
VPC4>ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
```

4. Pengujian Akses Remote SSH VPC to Router

Pengujian ini dilakukan untuk memastikan bahwa konfigurasi firewall filter yang disebut "block-ssh" berfungsi untuk memverifikasi firewall filter berhasil mencegah akses SSH dari luar jaringan ke router yang ditentukan.

- **VPC4 to R1**

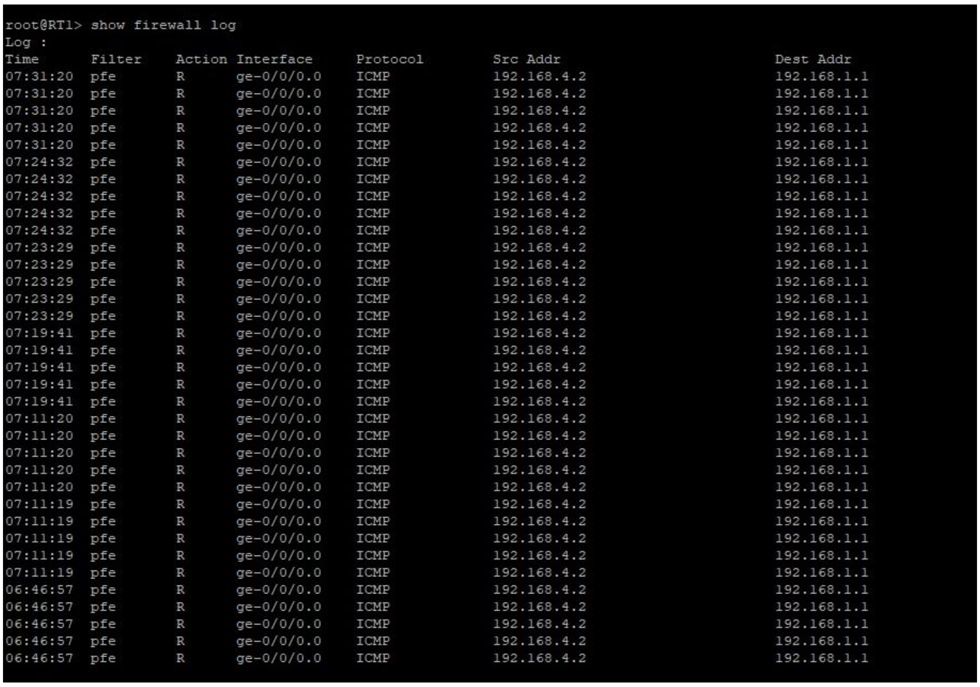


```
VPC4>ssh -l ftap.annisa 192.168.1.1
% Destination unreachable; gateway or host down
```

5. **Show Firewall Log**

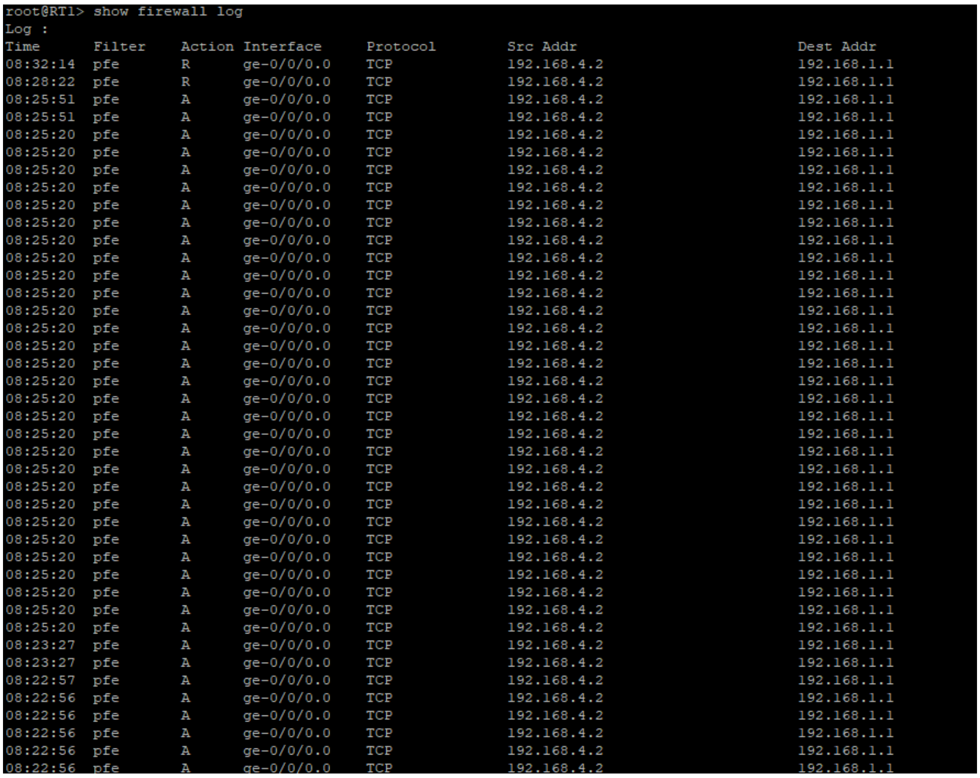
Perintah ini digunakan untuk melihat catatan log aktivitas firewall. Catatan ini menampilkan informasi tentang paket yang diterima atau ditolak oleh firewall. Pada kolom action “R” menandakan bahwa paket telah ditolak sedangkan untuk kolom action “A” menandakan bahwa paket diterima.

- **Blok Ping**



```
root@RT1> show firewall log
Log :
Time      Filter    Action Interface     Protocol        Src Addr                          Dest Addr
07:31:20  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:31:20  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:31:20  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:31:20  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:31:20  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:24:32  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:24:32  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:24:32  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:24:32  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:24:32  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:23:29  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:23:29  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:23:29  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:23:29  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:23:29  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:19:41  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:19:41  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:19:41  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:19:41  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:19:41  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:11:20  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:11:20  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:11:20  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:11:20  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:11:20  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:11:19  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:11:19  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:11:19  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:11:19  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
07:11:19  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
06:46:57  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
06:46:57  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
06:46:57  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
06:46:57  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
06:46:57  pfe       R      ge-0/0/0.0    ICMP            192.168.4.2                       192.168.1.1
```

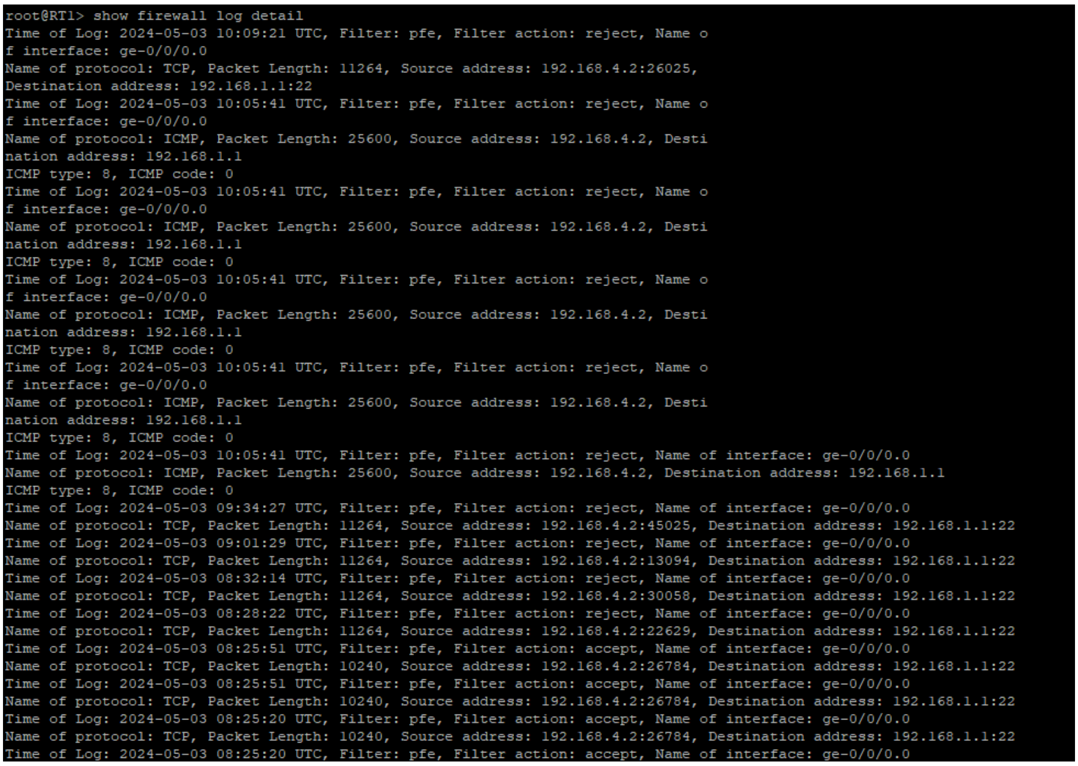
- **Blok SSH**



```
root@RT1> show firewall log
Log :
Time      Filter    Action Interface     Protocol        Src Addr                          Dest Addr
08:32:14  pfe       R      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:28:22  pfe       R      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:51  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:51  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:25:20  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:23:27  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:23:27  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:22:57  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:22:56  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:22:56  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:22:56  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:22:56  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
08:22:56  pfe       A      ge-0/0/0.0    TCP             192.168.4.2                       192.168.1.1
```

6. Show Firewall Log Detail

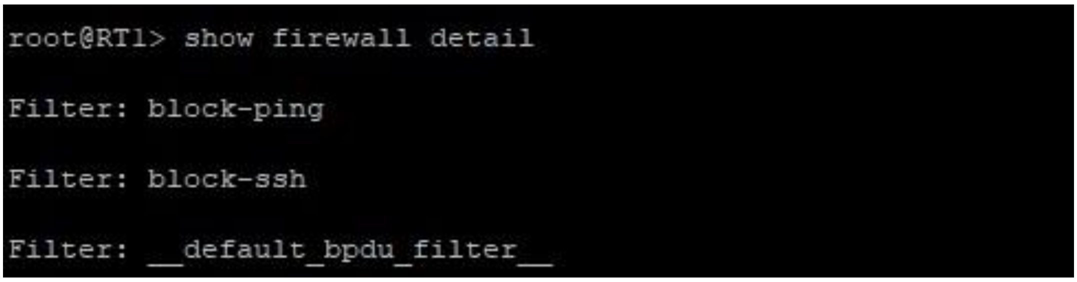
Perintah ini digunakan untuk menampilkan detail dari log aktivitas firewall dan mencakup informasi seperti waktu, jenis aksi (diterima atau ditolak), interface, protokol yang digunakan, IP source, dan IP destination.



```
root@RT1> show firewall log detail
Time of Log: 2024-05-03 10:09:21 UTC, Filter: pfe, Filter action: reject, Name o
f interface: ge-0/0/0.0
Name of protocol: TCP, Packet Length: 11264, Source address: 192.168.4.2:26025,
Destination address: 192.168.1.1:22
Time of Log: 2024-05-03 10:05:41 UTC, Filter: pfe, Filter action: reject, Name o
f interface: ge-0/0/0.0
Name of protocol: ICMP, Packet Length: 25600, Source address: 192.168.4.2, Desti
nation address: 192.168.1.1
ICMP type: 8, ICMP code: 0
Time of Log: 2024-05-03 10:05:41 UTC, Filter: pfe, Filter action: reject, Name o
f interface: ge-0/0/0.0
Name of protocol: ICMP, Packet Length: 25600, Source address: 192.168.4.2, Desti
nation address: 192.168.1.1
ICMP type: 8, ICMP code: 0
Time of Log: 2024-05-03 10:05:41 UTC, Filter: pfe, Filter action: reject, Name o
f interface: ge-0/0/0.0
Name of protocol: ICMP, Packet Length: 25600, Source address: 192.168.4.2, Desti
nation address: 192.168.1.1
ICMP type: 8, ICMP code: 0
Time of Log: 2024-05-03 10:05:41 UTC, Filter: pfe, Filter action: reject, Name o
f interface: ge-0/0/0.0
Name of protocol: ICMP, Packet Length: 25600, Source address: 192.168.4.2, Desti
nation address: 192.168.1.1
ICMP type: 8, ICMP code: 0
Time of Log: 2024-05-03 10:05:41 UTC, Filter: pfe, Filter action: reject, Name of interface: ge-0/0/0.0
Name of protocol: ICMP, Packet Length: 25600, Source address: 192.168.4.2, Destination address: 192.168.1.1
ICMP type: 8, ICMP code: 0
Time of Log: 2024-05-03 09:34:27 UTC, Filter: pfe, Filter action: reject, Name of interface: ge-0/0/0.0
Name of protocol: TCP, Packet Length: 11264, Source address: 192.168.4.2:45025, Destination address: 192.168.1.1:22
Time of Log: 2024-05-03 09:01:29 UTC, Filter: pfe, Filter action: reject, Name of interface: ge-0/0/0.0
Name of protocol: TCP, Packet Length: 11264, Source address: 192.168.4.2:13094, Destination address: 192.168.1.1:22
Time of Log: 2024-05-03 08:32:14 UTC, Filter: pfe, Filter action: reject, Name of interface: ge-0/0/0.0
Name of protocol: TCP, Packet Length: 11264, Source address: 192.168.4.2:30058, Destination address: 192.168.1.1:22
Time of Log: 2024-05-03 08:28:22 UTC, Filter: pfe, Filter action: reject, Name of interface: ge-0/0/0.0
Name of protocol: TCP, Packet Length: 11264, Source address: 192.168.4.2:22629, Destination address: 192.168.1.1:22
Time of Log: 2024-05-03 08:25:51 UTC, Filter: pfe, Filter action: accept, Name of interface: ge-0/0/0.0
Name of protocol: TCP, Packet Length: 10240, Source address: 192.168.4.2:26784, Destination address: 192.168.1.1:22
Time of Log: 2024-05-03 08:25:51 UTC, Filter: pfe, Filter action: accept, Name of interface: ge-0/0/0.0
Name of protocol: TCP, Packet Length: 10240, Source address: 192.168.4.2:26784, Destination address: 192.168.1.1:22
Time of Log: 2024-05-03 08:25:20 UTC, Filter: pfe, Filter action: accept, Name of interface: ge-0/0/0.0
Name of protocol: TCP, Packet Length: 10240, Source address: 192.168.4.2:26784, Destination address: 192.168.1.1:22
Time of Log: 2024-05-03 08:25:20 UTC, Filter: pfe, Filter action: accept, Name of interface: ge-0/0/0.0
```

7. Show Firewall Detail

Perintah ini digunakan untuk menampilkan detail konfigurasi firewall yang ada pada perangkat, misalnya seperti filter.



```
root@RT1> show firewall detail

Filter: block-ping

Filter: block-ssh

Filter: __default_bpdu_filter__
```