

Packet Debugging pada Router Firewall Juniper SSG140

Author : Antonius Robotsoft

www.robotsoft.co.id – www.freenergi.com – www.jasaplus.com

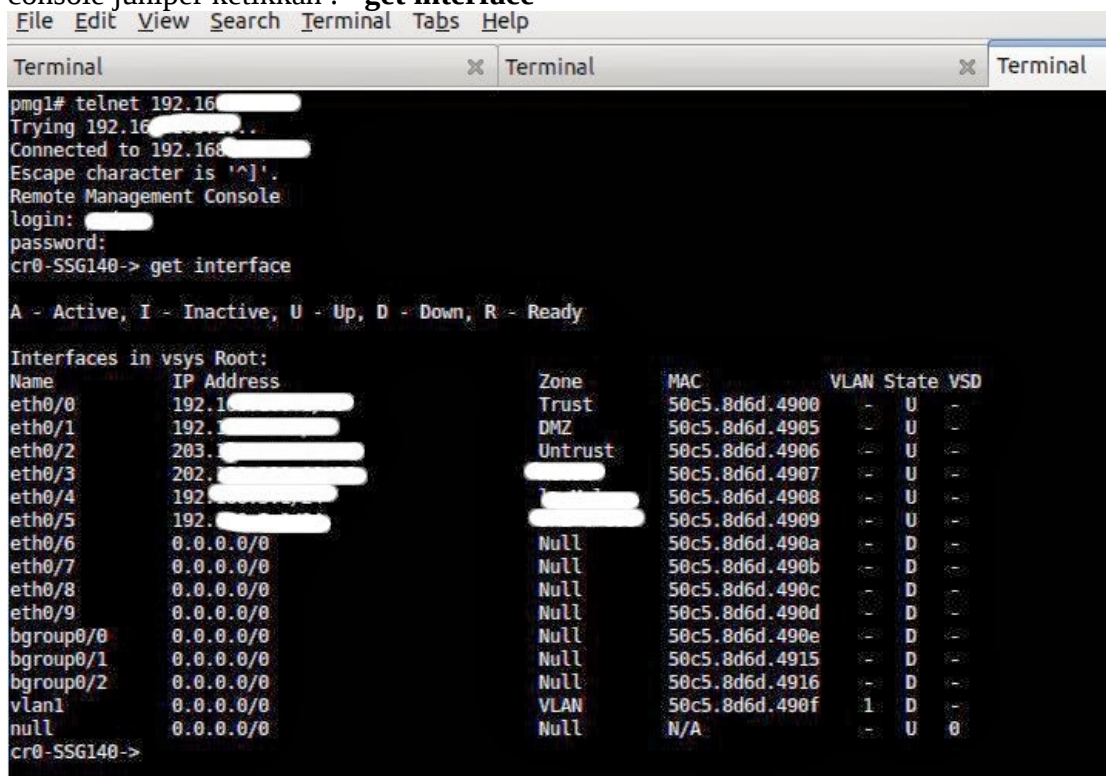
github : <https://github.com/antoniusrobotsoft>

Juniper SSG140 biasanya digunakan untuk jaringan dengan skala kecil hingga medium sebagai router firewall. Perangkat ini mendukung : dual stack ip versi 4, ip versi 6 firewall, deteksi syn flood, BGP, IPsec VPN, proteksi ddos dan implementasi UTM seperti : anti virus , anti spam.

Juniper SSG140 memiliki fitur debugging yang memungkinkan kita melihat paket yang lalu lalang melalui router ini. Ada 2 modus pada router ini :

"Flow level debugging" (digunakan untuk trafik umum) dan **"Flow Tunnel debugging"** (digunakan untuk trafik ipsec).

Pada contoh kali ini, mari kita lihat dulu seluruh interface sebelum melakukan capture paket, Pada console juniper ketikkan : **"get interface"**



```
File Edit View Search Terminal Tabs Help
Terminal x Terminal x Terminal
pmg1# telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Remote Management Console
login:
password:
cr0-SSG140-> get interface

A - Active, I - Inactive, U - Up, D - Down, R - Ready

Interfaces in vsys Root:
Name      IP Address      Zone      MAC      VLAN State VSD
eth0/0    192.168.1.1     Trust     50c5.8d6d.4900  -   U
eth0/1    192.168.1.2     DMZ       50c5.8d6d.4905  -   U
eth0/2    203.113.1.1     Untrust   50c5.8d6d.4906  -   U
eth0/3    202.113.1.1     -         50c5.8d6d.4907  -   U
eth0/4    192.168.1.3     -         50c5.8d6d.4908  -   U
eth0/5    192.168.1.4     -         50c5.8d6d.4909  -   U
eth0/6    0.0.0.0/0       Null      50c5.8d6d.490a  -   D
eth0/7    0.0.0.0/0       Null      50c5.8d6d.490b  -   D
eth0/8    0.0.0.0/0       Null      50c5.8d6d.490c  -   D
eth0/9    0.0.0.0/0       Null      50c5.8d6d.490d  -   D
bgroup0/0 0.0.0.0/0       Null      50c5.8d6d.490e  -   D
bgroup0/1 0.0.0.0/0       Null      50c5.8d6d.4915  -   D
bgroup0/2 0.0.0.0/0       Null      50c5.8d6d.4916  -   D
vlan1     0.0.0.0/0       VLAN     50c5.8d6d.490f  1   D
null      0.0.0.0/0       Null      N/A             -   U 0
cr0-SSG140->
```

Dari gambar di atas, kita bisa melihat daftar seluruh interface, prefix ip dan zona2nya. Pada contoh di atas, kita memiliki :

trusted zone, untrusted, and DMZ (demilitarized zone).

Menggunakan Flow Filter untuk Capture Trafik

Pada contoh kali ini, kita akan melakukan capture dengan filtering yang khusus untuk menangkap

incoming packet ke destination address

Ketikkan di console juniper : **"set ff dst-ip 192.168.100.18 dst-port 80"**

Lalu kita akan mulai capture, ketikkan pada console ssg140 :
"debug flow basic"

Jika Anda ingin melihat modus debug yang sedang digunakan ketikkan :
"get debug"

Untuk melakukan dump hasil debugging paket ketikkan :
"get db str"

Di bawah ini adalah contoh hasilnya :

```
File Edit View Search Terminal Tabs Help
Terminal x Terminal
^--command not completed
cr0-SSG140-> set ff dst-ip 192.168.100.18 dst-port 80
filter added
cr0-SSG140-> debug flow basic
cr0-SSG140-> get db str
111. [REDACTED] 24452,6<Root>
existing session found. sess token 3
flow got session.
flow session id 46799
flow_main_body_vector in ifp ethernet0/0 out ifp N/A
flow_vector index 0x113, vector addr 0x3e97e74, orig vector 0x3e97e74
tcp seq check.
post addr xlation: 203. [REDACTED] -> 111. [REDACTED]
packet send out to 02a3836322a7 through ethernet0/2
***** 397781.0: <Trust/ethernet0/0> packet received [654]*****
ipid = 386(0182), @1d51a114
packet passed sanity check.
flow decap vector IPv4 process
ethernet0/0:192.168.100.18/80->111. [REDACTED] /60607,6<Root>
existing session found. sess token 3
flow got session.
flow session id 46461
flow_main_body_vector in ifp ethernet0/0 out ifp N/A
flow_vector index 0x113, vector addr 0x3e97e74, orig vector 0x3e97e74
tcp seq check.
post addr xlation: 203. [REDACTED] -> 111. [REDACTED]
packet send out to 02a3836322a7 through ethernet0/2
***** 397781.0: <Trust/ethernet0/0> packet received [486]*****
ipid = 387(0183), @1d5ef914
packet passed sanity check.
flow decap vector IPv4 process
ethernet0/0:192.168.100.18/80->111. [REDACTED] /6982,6<Root>
existing session found. sess token 3
flow got session.
flow session id 47077
flow_main_body_vector in ifp ethernet0/0 out ifp N/A
flow_vector index 0x113, vector addr 0x3e97e74, orig vector 0x3e97e74
tcp seq check.
post addr xlation: 203. [REDACTED] -> 111. [REDACTED]
packet send out to 02a3836322a7 through ethernet0/2
***** 397781.0: <Trust/ethernet0/0> packet received [476]*****
ipid = 388(0184), @1d573914
packet passed sanity check.
--- more ---
```

Pada Flow session id 4679, kita bisa melihat adanya trafik yang lewat melalui interface ethernet0/0 (eth0/0) pada ip prefix : 192.168.*****/* (Trusted Zone kita), di mana paket dikirimkan keluar melalui interface ethernet0/2.