AIX Simple Firewall

Prerequisities

Packages to be installed

- bos.msg.en_US.net.ipsec
- bos.net.ipsec.keymgt
- bos.net.ipsec.rte
- clic.rte.kernext
- clic.rte.lib

CLI

```
lslpp -l bos.msg.en_US.net.ipsec

  Fileset                      Level  State      Description
  ----------------------------------------------------------------------------
Path: /usr/lib/objrepos
  bos.msg.en_US.net.ipsec     7.2.5.0  COMMITTED  IP Security Messages - U.S.
                                                  English
```

Start/Stop IP Security

CLI

```
# Start command for ipsec_v4
/usr/sbin/mkdev -c ipsec -t 4
/usr/sbin/mkfilt -v 4 -u -z P

# Stop command
/usr/sbin/rmdev -l ipsec_v4
```

Smitty

`smitty ipsec4` > Start/Stop IP Security > Start IP Security

- Start IP Security: [Now and After Reboot]

- Deny All Non_Secure IP Packets: [no]

Verify command

```
lsdev -C | grep ipsec
lsdev -l ipsec_v4


ipsec_v4 Available  IP Version 4 Security Extension
```

?????

```
cp /etc/syslog.conf /etc/syslog.conf.bak
echo "local4.debug /var/log/ipsec.log" >> /etc/syslog.conf
touch /var/log/ipsec.log
chmod 0644 /var/log/ipsec.log
refresh -s syslogd
```


```
cp /etc/syslog.conf /etc/syslog.conf.bak
echo "local4.debug /var/log/ipsec.log" >> /etc/syslog.conf
touch /var/log/ipsec.log
chmod 0644 /var/log/ipsec.log
refresh -s syslogd
```


??/??????

- ??????????????????????????? filesystem??????????
- ?????????? Logging control?

```
# Start the packet logging
mkfilt -v4 -g start


# Stop the packet logging
mkfilt -v4 -g stop
```

Filter Rules

?????

- genfilt : ????
- rmfilt : ????
  - `rmfilt -v 4 -n 3` : ???? 3

- chfilt : ????
  - `chfilt -v 4 -n 3 -s xxx.xxx.xxx.xxx` : ????3 ??? IP
- ?????? : `mkfilt -v 4 -u`
- ?????? : `mkfilt -v 4 -d`
- ?????? : `lsfilt -v 4 -O`

?????

- `-v 4` : IPv4 ??
- `-a` : Action?P (Permit), D (Deny)
- `-n` : ????
- `-s` : ?? IP ?????? 192.168.99.1 ? 192.168.99.0
- `-m` : ??????? IP ? 255.255.255.255?C ?? IP ? 255.255.255.0
- `-d` : ?? IP ?????? 192.168.99.1 ? 192.168.99.0
- `-M` : ??????? IP ? 255.255.255.255?C ?? IP ? 255.255.255.0
- `-g` : source routing, ?? N, Y(default)
- `-c` : Protocol, ?? tcp, udp, all
- `-O eq -P 21` : Port 21 (FTP)
- `-O any -P 0` : ?? Port (????)
- `-w` : Direction, ?? I (inbound), O (outbound) ? B (both)
- `-l` : ??????????? Y, N(default) (?????????)
- `-i` : ??????? all, en0
- `-D` : Description, ??????

?????

Inbound Rule : ?? FTP (port 21) ?????? IP (my-linux-ip) ????

```
genfilt -v 4 -a P -s <my-linux-ip> -m 255.255.255.255 -d <aix-server-IP> -M 255.255.255.255 -g Y -c tcp -o any -p 0 -O eq -P 21 -r B -w I -l Y -f Y -i all


genfilt -v 4 -a D -s 0.0.0.0 -m 0.0.0.0 -d <aix-server-IP> -M 255.255.255.255 -g Y -c tcp -o any -p 0 -O eq -P 21 -r B -w I -l N -f Y -i all
```

- Rule 0,1,2 ???????
- TIPs
  - ??????????????
  - ??????? Permit ?????? Deny ????

```
root@aixvm:> lsfilt -v4 -O


1|permit|0.0.0.0|0.0.0.0|0.0.0.0|0.0.0.0|no|udp|eq|4001|eq|4001|both|both|no|all packets|0|all|0|||Default Rule
2|*** Dynamic filter placement rule for IKE tunnels ***|no
```

3|permit|192.168.99.1|255.255.255.255|192.168.99.100|255.255.255.255|yes|tcp|any|0|eq|21|both|inbound|yes|all packets|0|all|0|||
4|deny|0.0.0.0|0.0.0.0|192.168.99.100|255.255.255.255|yes|tcp|any|0|eq|21|both|inbound|no|all packets|0|all|0|||
0|permit|0.0.0.0|0.0.0.0|0.0.0.0|0.0.0.0|yes|all|any|0|any|0|both|both|no|all packets|0|all|0|||Default Rule

root@aixvm:> lsfilt -v4
Beginning of IPv4 filter rules.
Rule 1:
Rule action : permit
Source Address : 0.0.0.0
Source Mask : 0.0.0.0
Destination Address : 0.0.0.0
Destination Mask : 0.0.0.0
Source Routing : no
Protocol : udp
Source Port : eq 4001
Destination Port : eq 4001
Scope : both
Direction : both
Logging control : no
Fragment control : all packets
Tunnel ID number : 0
Interface : all
Auto-Generated : yes
Expiration Time : 0
Description : Default Rule

Rule 2:
*** Dynamic filter placement rule for IKE tunnels ***
Logging control : no

Rule 3:
Rule action : permit
Source Address : 192.168.99.1
Source Mask : 255.255.255.255
Destination Address : 192.168.99.100
Destination Mask : 255.255.255.255
Source Routing : yes
Protocol : tcp

Source Port : any 0
Destination Port : eq 21
Scope : both
Direction : inbound
Logging control : yes
Fragment control : all packets
Tunnel ID number : 0
Interface : all
Auto-Generated : no
Expiration Time : 0
Description :

Rule 4:
Rule action : deny
Source Address : 0.0.0.0
Source Mask : 0.0.0.0
Destination Address : 192.168.99.100
Destination Mask : 255.255.255.255
Source Routing : yes
Protocol : tcp
Source Port : any 0
Destination Port : eq 21
Scope : both
Direction : inbound
Logging control : no
Fragment control : all packets
Tunnel ID number : 0
Interface : all
Auto-Generated : no
Expiration Time : 0
Description :

Rule 0:
Rule action : permit
Source Address : 0.0.0.0
Source Mask : 0.0.0.0
Destination Address : 0.0.0.0
Destination Mask : 0.0.0.0
Source Routing : yes
Protocol : all

```
Source Port         : any 0
Destination Port    : any 0
Scope               : both
Direction           : both
Logging control     : no
Fragment control    : all packets
Tunnel ID number    : 0
Interface           : all
Auto-Generated      : no
Expiration Time     : 0
Description         : Default Rule

End of IPv4 filter rules.
```

????

?? 3 ? 4 ????

```
...
3|deny|0.0.0.0|0.0.0.0|192.168.99.100|255.255.255.255|yes|tcp|any|0|eq|21|both|inbound|no|all packets|0|all|0|||
4|permit|192.168.99.1|255.255.255.255|192.168.99.100|255.255.255.255|yes|tcp|any|0|eq|21|both|inbound|yes|all packets|0|all|0|||
...
```

???

1. ??? 4 ??`rmfilt -v4 -n 3`
2. ?????????????? 3?`genfilt -v 4 -n 3 -a P -s 192.168.99.1 -m 255.255.255.255 -d 192.168.99.100 -M 255.255.255.255 -g Y -c tcp -o any -p 0 -O eq -P 21 -r B -w I -l Y -f Y -i all`

????

??????????????????

```
rmfilt -v4 -n all
```

??/????

??

- ??? `expfilt -r -f .`
- `-f .` : *????????????? ipsec_fltr_rule.exp*
- `-r` : *????????????? Direction ????*

```
root@aixvm:ipsec_filters> lsfilt -v4 -O

1|permit|0.0.0.0|0.0.0.0|0.0.0.0|0.0.0.0|no|udp|eq|4001|eq|4001|both|both|no|all packets|0|all|0|||Default Rule
2|*** Dynamic filter placement rule for IKE tunnels ***|no
3|permit|192.168.99.8|255.255.255.255|192.168.99.100|255.255.255.255|yes|tcp|any|0|eq|21|both|inbound|yes
|all packets|0|all|0|||
4|deny|0.0.0.0|0.0.0.0|192.168.99.100|255.255.255.255|yes|tcp|any|0|eq|21|both|inbound|no|all
packets|0|all|0|||
0|permit|0.0.0.0|0.0.0.0|0.0.0.0|0.0.0.0|yes|all|any|0|any|0|both|both|no|all packets|0|all|0|||Default Rule

root@aixvm:ipsec_filters> expfilt -r -f .

Filter rule 3 for IPv4 has been exported successfully.
Filter rule 4 for IPv4 has been exported successfully.
Filter rule(s) have been exported to ipsec_fltr_rule.exp successfully.

root@aixvm:ipsec_filters> ls -l
total 16
-rw-r--r--    1 root     system          417 Jun 03 15:37 ipsec_fltr_rule.exp
```

??

- ??? `impfilt -f .` ???????

```
root@aixvm:ipsec_filters> ls -l
total 16
-rw-r--r--    1 root     system          417 Jun 03 15:37 ipsec_fltr_rule.exp

root@aixvm:ipsec_filters> lsfilt -v4 -O
1|permit|0.0.0.0|0.0.0.0|0.0.0.0|0.0.0.0|no|udp|eq|4001|eq|4001|both|both|no|all packets|0|all|0|||Default Rule
2|*** Dynamic filter placement rule for IKE tunnels ***|no
3|permit|192.168.99.8|255.255.255.255|192.168.99.100|255.255.255.255|yes|tcp|any|0|eq|21|both|inbound|yes
|all packets|0|all|0|||
4|deny|0.0.0.0|0.0.0.0|192.168.99.100|255.255.255.255|yes|tcp|any|0|eq|21|both|inbound|no|all
packets|0|all|0|||
0|permit|0.0.0.0|0.0.0.0|0.0.0.0|0.0.0.0|yes|all|any|0|any|0|both|both|no|all packets|0|all|0|||Default Rule
```

```
root@aixvm:ipsec_filters> rmfilt -v4 -n all
Filter rule 3 for IPv4 has been removed successfully.
Filter rule 4 for IPv4 has been removed successfully.

root@aixvm:ipsec_filters> impfilt -f .
Filter rule 3 for IPv4 imported as rule 3.
Filter rule 4 for IPv4 imported as rule 4.
Filter rule(s) have been imported successfully.

root@aixvm:ipsec_filters> lsfilt -v4 -O
1|permit|0.0.0.0|0.0.0.0|0.0.0.0|0.0.0.0|no|udp|eq|4001|eq|4001|both|both|no|all packets|0|all|0|||Default Rule
2|*** Dynamic filter placement rule for IKE tunnels ***|no
3|permit|192.168.99.8|255.255.255.255|192.168.99.100|255.255.255.255|yes|tcp|any|0|eq|21|both|inbound|yes
|all packets|0|all|0|||
4|deny|0.0.0.0|0.0.0.0|192.168.99.100|255.255.255.255|yes|tcp|any|0|eq|21|both|inbound|no|all
packets|0|all|0|||
0|permit|0.0.0.0|0.0.0.0|0.0.0.0|0.0.0.0|yes|all|any|0|any|0|both|both|no|all packets|0|all|0|||Default Rule
```

?????

Rule:

- action: deny
- source: 192.168.99.1
- destination: any
- protocol: all
- direction: inbound

```
genfilt -v 4 -a D -s 192.168.99.1 -m 255.255.255.255 -d 0.0.0.0 -M 0.0.0.0 -g Y -c all -r B -w I -l Y -f Y -i all
```

Revision #33
Created 2 June 2025 10:00:03 by Admin
Updated 3 June 2025 17:49:45 by Admin